

May and August 2024
Strategic Case Study
2019 CGMA Professional Qualification
Full post exam support materials

Below are the full post-exam supporting materials for the Strategic Case Study Exam. Use the links on this page to jump to the documents required.

Pre-seen material

May and August Strategic Case Study [pre-seen](#).

Examiner's report

The May and November 2024 [examiner's report](#).

Exam variants

- [Variant 1](#)
- [Variant 2](#)
- [Variant 3](#)
- [Variant 4](#)
- [Variant 5](#)
- [Variant 6](#)

Suggested solutions

- [Suggested solutions for variant 1](#)
- [Suggested solutions for variant 2](#)
- [Suggested solutions for variant 3](#)
- [Suggested solutions for variant 4](#)
- [Suggested solutions for variant 5](#)
- [Suggested solutions for variant 6](#)

Marking Guidance

- [Marking guidance for variant 1](#)
- [Marking guidance for variant 2](#)
- [Marking guidance for variant 3](#)
- [Marking guidance for variant 4](#)
- [Marking guidance for variant 5](#)
- [Marking guidance for variant 6](#)

If you need any further information please [contact us](#).

Strategic Case Study Examination

May - August 2024

Pre-seen material

SEFWELL

Context Statement

We are aware that there has been, and remains, a significant amount of change globally. To assist with clarity and fairness, we do not expect students to factor these changes in when responding to, or preparing for, case studies. This pre-seen, and its associated exams (while aiming to reflect real life), are set in a context where current and on-going global issues have not had an impact.

Remember, marks in the exam will be awarded for valid arguments that are relevant to the question asked. Answers that make relevant references to current affairs will, of course, be marked on their merits.

Contents

Introduction	2
Security industry	3
Physical security services	5
Intelligence-led services	6
Saefwell	7
Extracts from Saefwell's annual report	11
Saefwell's Board of directors	11
Board responsibilities	13
Saefwell's Principal Risks	14
Extract from competitor's financial statements	17
Share price history	19
News stories	20

Introduction

Saefwell is a quoted company that offers advice and support on corporate security and enterprise risk management. The company offers a number of different services, ranging from the provision of security guarding to consulting on enterprise risk management. Consultancy activities range from advising on systems to counter security threats (both physical and cyber) to the provision of intelligence and investigations intended to address evolving threats.




You are a senior manager in Saefwell's finance function. You report directly to the Board and advise on special projects and strategic matters.

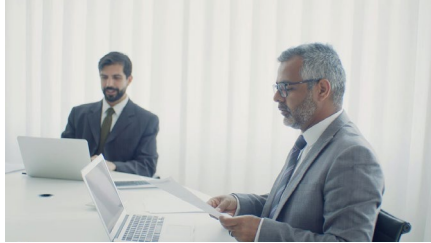



Saefwell operates on a global basis, with regional offices in several countries. Its head office is in Barrland, a developed country that has an active and well-regulated stock exchange. Barrland's currency is the B\$. Barrland requires companies to prepare their financial statements in accordance with International Financial Reporting Standards (IFRS).

Security industry

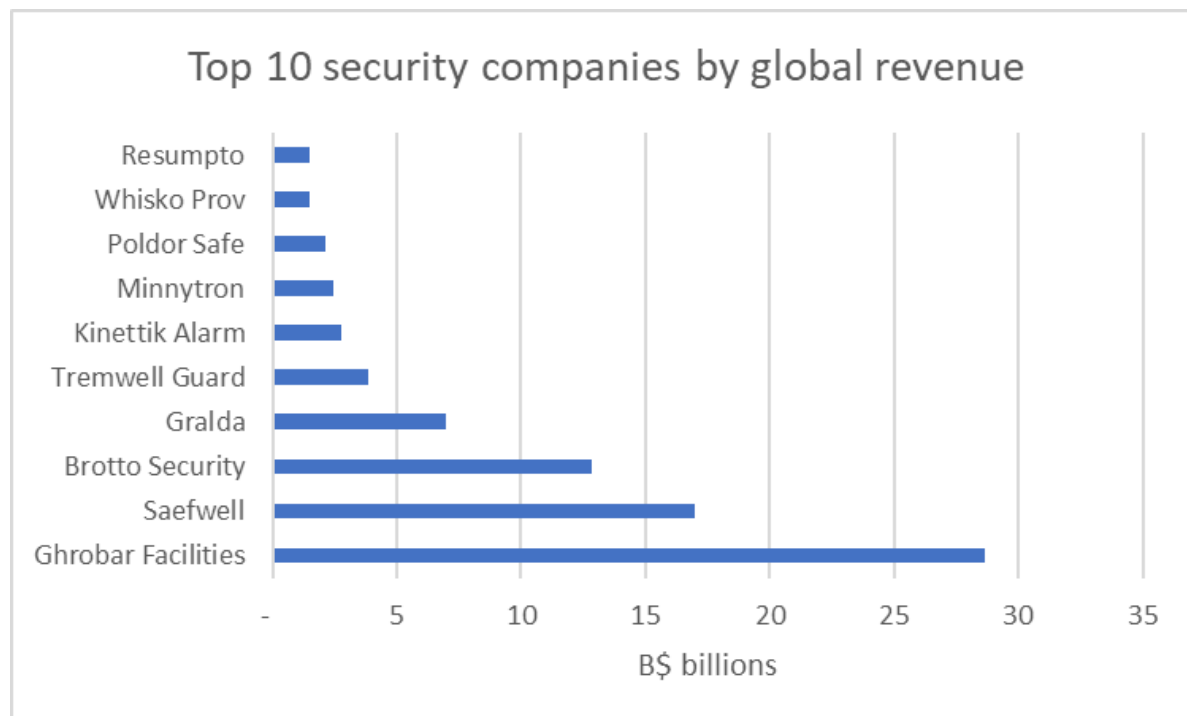
The modern-day security industry dates back to the middle of the 19th century. Previously, security companies provided little more than physical protection for individuals and for property. By the mid-1800s, security companies started to offer intelligence-led services, primarily focussing on protecting clients from loss. These services included counter-espionage and fraud investigation.

Typically, a major security company will offer some or all of the following services:

On-site guarding 	<p>Clients often outsource their physical security arrangements to security companies.</p> <p>On-site guarding can take several forms, including:</p> <ul style="list-style-type: none">• Staffing reception desks and other entrances, checking visitors' credentials.• Patrolling clients' premises, detecting intruders.• Providing security staff for retail shops, either in uniform or in plain clothes, to discourage theft of goods. <p>Security staff report any suspected criminal activity to the police. They do not have law enforcement powers.</p>
Mobile guarding 	<p>Mobile guarding uses vehicle patrols to visit client premises at random intervals while they are unoccupied. Security guards check that doors are locked and that there are no signs of forced entry.</p> <p>Guards check in by phone or radio to confirm that a check has been undertaken and that everything is secure.</p>
Remote services 	<p>Clients can pay to have their electronic security systems monitored when their premises are unoccupied. Security companies have control rooms that receive any notifications of intrusion from client systems.</p> <p>Staff are trained to respond to any alarms, usually by notifying both the police and a designated contact, such as a manager who has a key to the property.</p>

<p>Corporate investigations</p> 	<p>Most large security companies can carry out specific investigations tailored to a client's needs. For example:</p> <ul style="list-style-type: none"> • Counter-espionage, including the investigation of suspicions that intellectual property has been copied and is being abused by a third party. • Fraud investigations, including the collection of evidence relating to suspicions that an employee or other stakeholder has defrauded the company. • Vetting potential appointees, such as individuals who are being considered for appointment to senior positions within an organisation. These investigations will involve a thorough investigation of that person's background and character. <p>Security companies employ trained investigators to carry out these assignments.</p>
<p>Risk management</p> 	<p>Security companies can provide consultancy support, advising management concerning strategic risks, both in terms of identification and mitigation.</p> <p>Security companies compete with other consultants, such as management consultancies, for such work. Security companies generally focus on risk management and the development of controls and other procedures for the management of risks.</p>
<p>Security assessment</p> 	<p>Security companies are often asked to evaluate existing corporate security systems, both physical security and cyber security. Such evaluations can be based on the study of the systems that are in place or they can involve attempts to breach systems through the identification and exploitation of weaknesses.</p>
<p>Training</p> 	<p>Security companies can provide courses for management and staff at all levels within the organisation, ranging from practical training for the client's security guards to training in enterprise risk management for senior managers and board members.</p>

Some security companies combine security services with facilities management, rather than focussing exclusively on security services. For example, Ghrobar Facilities provides its clients with a wide variety of services such as cleaning and property maintenance, in addition to on-site guarding, mobile guarding and remote services. Saefwell has the second-highest global revenues of all security companies.



Some security companies specialise in intelligence-led services. Resumpto, Whisko Prov and Poldor Safe focus on advising and training clients.

Minnytron, Kinettik Alarm and Tremwell Guard focus on protecting client staff and property, through on-site guarding, mobile guarding and remote services.

Gralda, Brotto Security and Saefwell focus on security, offering both physical protection and intelligence-led security.

Physical security services

Physical security services involve the provision of trained staff to undertake one or more security duties. These range from staffing the reception areas in clients' offices, checking the credentials of staff and visitors seeking entry, to the provision of roving patrols in warehouses and factories, asking potential intruders to explain their presence.

Many countries have legislation that requires security staff to be licensed if they are employed to carry out "front-line" work on behalf of third parties. Licences are required for:

- guarding property against theft, damage or unauthorised access
- operating surveillance equipment, such as closed-circuit television (CCTV) feeds, to guard premises or protect people from assault
- holding keys on behalf of third parties.

Licences are granted to applicants who have completed an approved training course and have passed the course assessments. The government's licensing authority then carries out a criminal record check, which confirms that applicants for licences have not been convicted of offences that are inconsistent with security work, such as crimes involving dishonesty or

violence. Licence holders must inform the licensing authority if they are charged or convicted of a criminal offence.

Licences are not normally required for security staff who are employed directly by the company that uses their services.

Global security companies such as Saefwell and Ghrobar Facilities tend to restrict their provision of physical security services to countries where their staff are unlikely to be at serious risk of physical harm. Their security staff are not expected to carry weapons such as firearms, pepper spray and batons.

Security staff do not have the same powers as police officers. Police officers have the power to arrest individuals if they have reasonable grounds to believe that they have committed criminal offences. Most security companies train their staff to contact the police if they suspect that a crime is being committed and to observe and record events from a safe distance where possible. Security staff are not normally expected to use force to subdue a thief or attacker. The law does, however, permit all citizens, regardless of whether they are employed in a security role, to use reasonable force when acting in self-defence or when apprehending criminals who would otherwise escape justice.

Security companies carry out their own risk assessments before committing staff. They may refuse to accept assignments that would place staff in physical danger unless that danger can be mitigated through training or the adoption of safe working practices. For example, staff being asked to patrol warehouses where goods are being loaded and unloaded should be issued with high visibility jackets, safety helmets and steel-toed work boots to reduce the risk of injury in that environment. Reception staff in city centre offices may require little more than uniforms that identify them as security staff and radios with which to summon assistance.

Intelligence-led services

Intelligence-led services tend to require specialist consultants. Clients will usually be seeking advice on specific matters that require considerable expertise.

For example, a client might want some reassurance that its security systems are effective and could ask a security company to attempt to gain access without being detected. That could involve using a team of security experts to use the same techniques that would be employed by criminals or unscrupulous business rivals to gain unauthorised access. Evidence of weaknesses might then be presented to senior management, perhaps by showing them photographs of sensitive documents.

Clients might make a similar request to test the security of online systems. Again, consultants would apply the same techniques used by hackers in order to attempt to access or disrupt the operation of clients' IT systems. The objective of such an exercise is hopefully to confirm that the targeted systems and files are not vulnerable, although a successful attempt to hack the system will alert the client as to the system's shortcomings and allow a solution to be developed.

Assignments may be relatively unstructured. For example, a client may be considering locating a new factory in a foreign country that is emerging as an inexpensive location in which to do business. The client may be concerned about both the financial risks associated with investing in this country and the health and safety risks associated with asking managers and staff to base themselves there. A security company might use a combination of desk research and site visits to investigate the risks and to provide the client with a report on the political, economic and health and safety risks.

Security companies recruit consulting staff from a variety of different backgrounds, taking account of the services that they offer and the associated skills that are required. Training and experience from disciplines such as auditing will be useful in ensuring that staff can offer

expertise in areas such as IT security and fraud investigation. Some assignments also require strong interpersonal skills. For example, the easiest way to enter a secure site is to persuade a security guard to permit access. If consultants can trick guards into letting them in, then so can intruders. Similarly, hackers often ask members of staff for their usernames and passwords and use these to access IT systems.

Intelligence-led security services tend to focus on strategic or governance matters and are intended to provide clients' boards with the assurance that they require with regard to strategic or governance risks. The open-ended nature of the work that these firms can undertake often puts them in competition with management consultants, accountancy firms and other professional entities.

Saefwell


Saefwell was founded in 1920 as a security company, specialising in providing guards to protect clients' premises. The company continues to offer physical security services, currently employing 460,000 security staff worldwide, operating in 74 countries.



Saefwell has been a major provider of intelligence-led risk management services since the 1970s. The company now employs 22,000 risk management consultants, most of whom are based in the company's head office in Barrland's Capital City and at four regional offices around the world. Risk management consultants expect to travel to assignments, enabling the company to provide almost worldwide coverage for its intelligence-led services. Saefwell has completed consultancy and training projects in 132 countries over the past 20 years.

The company was quoted on the Barrland Stock Exchange in 1991.

Saefwell provides its own training programmes for security guards, ensuring that all exceed the minimum requirements for licensing purposes in their home countries. The company provides ongoing training to ensure that all security staff are aware of their responsibilities and can fulfil those in a safe and professional manner. Saefwell also pays well, exceeding competitor's hourly rates of pay by as much as 10%.

Saefwell provides the following physical security services:

Reception 	<p>Large office buildings usually have security measures in place to ensure that only employees and legitimate visitors can obtain access. Those measures might include requiring staff to operate a gate using their staff pass or identity card and asking visitors to sign in at a reception desk, where they are given temporary passes after having their credentials checked.</p> <p>Saefwell uses experienced staff to provide reception services because intruders could gain access to sensitive information and could pose a threat to senior managers.</p>
Site security	<p>Companies often employ security guards to protect factories and storage sites to prevent theft and safeguard staff. Procedures can include checking the credentials of employees and visitors who wish to access the site, checking vehicle loads to ensure that despatches of goods have been authorised and patrolling sites to check that everything is in order.</p>

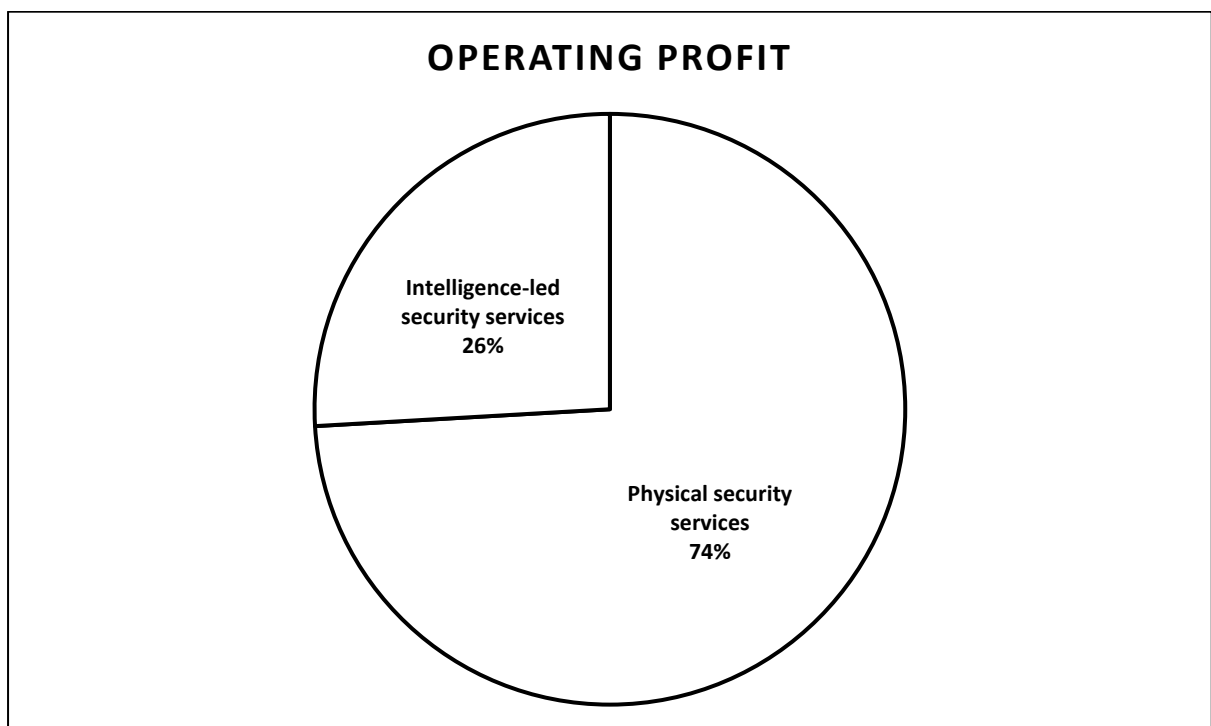
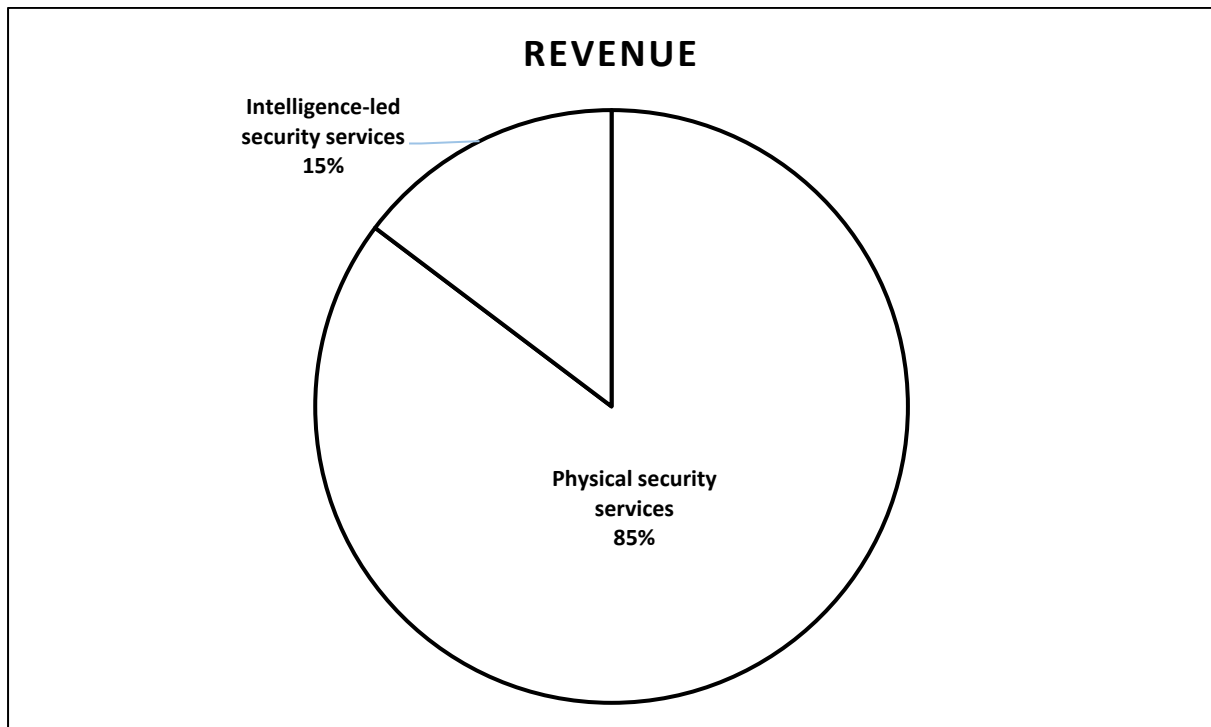
	<p>Many of Saefwell's site security staff have previously served in the military and have the ability to use their initiative when faced with a challenge.</p>
<p>Retail security</p> 	<p>Supermarkets and other large retailers can lose significant amounts of goods, and therefore revenue, due to theft by shoppers and shop staff. Saefwell can provide support by providing teams of security staff to deter theft. Security officers can be uniformed in order to provide visible deterrence or dressed in plain clothes to mingle with customers in order to watch covertly for theft.</p> <p>Saefwell's shop security staff are trained to gather evidence that can be used to prosecute thieves. They call the police when they identify cases of theft.</p>

Saefwell provides the following intelligence-led security services:

<p>Risk advisory service</p>	<p>Saefwell's clients often seek independent advice on the risks associated with strategic business decisions. External specialist consultants might be better informed about potential risks and may be able to alert the board to risks that have been overlooked.</p> <p>Saefwell maintains a detailed database of the threat profiles associated with doing business in 97 countries and so can advise on strategic risks associated with international expansion, either through investment or by conducting new business with foreign suppliers or customers.</p> <p>Saefwell's consultants are also experienced in developing risk assessments associated with other factors, such as entering new industries or launching new products.</p> <p>The firm has considerable expertise in gathering information from online sources, including social media and the dark web. If requested, Saefwell's consultants can determine whether there is any reason to believe that the client's business is under</p>
-------------------------------------	---

	<p>threat. For example, there could be indications that environmentalists have targeted a client for protests.</p>
Corporate investigations	<p>Saefwell can plan and conduct a tailored investigation to address any concerns that clients have with respect to operations or business relationships.</p> <p>Investigations can focus on a wide range of possible issues:</p> <ul style="list-style-type: none"> • Suspected fraud by a member of staff. Fraud investigations may seek to identify the culprit if assets have gone missing. Clients may also have a clear idea of the identity of a fraudster but wish to gather evidence that would justify dismissal or the pursuit of criminal charges. • The accuracy of information provided in the course of a business relationship, such as checking whether royalty payments are being made in full. • Investigating the accuracy of information provided by a key job applicant, including the validity of claims about education and prior work experience.
Penetration testing	<p>Saefwell's consultants can evaluate clients' security systems, both physical and online.</p> <p>Security checks can involve documenting and reviewing control systems, looking for weaknesses and advising on improvements.</p> <p>Penetration tests of IT systems can involve the use of social engineering to obtain access to clients' systems. For example, consultants might attempt to trick staff into revealing their IT system login details. Systems are clearly at risk if they succeed.</p>
Training	<p>Saefwell's consultants are frequently asked to provide training to update technical skills and knowledge of clients' managers in roles that involve risk management.</p> <p>Clients also seek training to inform and equip senior managers and directors who have responsibility for supervising controls and risk management procedures.</p> <p>All of Saefwell's consultants have the necessary skills to facilitate training courses in their areas of expertise. Using its consultants in this role enables Saefwell to ensure that its training courses make the best possible use of its consultants' experience.</p>

Saefwell relies on both physical and intelligence-led security services. The following analysis is based on the company's financial performance for the financial year ended 31 December 2023:



Extracts from Saefwell's annual report

Saefwell's mission, vision and values

Our mission

Saefwell's mission is to provide clients with the security solutions and services that they require in order to be able to focus on their core businesses.

Our vision

Saefwell's vision is to be the security industry's most trusted service provider.

Our values

- Saefwell is responsive.
- Saefwell is innovative.
- Saefwell treats its employees with respect and cares about their safety.

Saefwell's Board of directors

Dr Pratima Thakali, Non-Executive Chair

Pratima holds a doctorate in finance. She had a successful career in banking, including a period in which she served as chief executive for a major commercial bank. She retired from banking in 2020, joining Capital City University as a visiting professor in banking and financial services.

Pratima joined Saefwell as Non-Executive Chair in 2022.

Greg Hainge, Chief Executive Officer (CEO)

Greg is a qualified accountant. He trained as an auditor with a large accountancy firm, rising to the position of that firm's managing partner for Barrland. Greg left the firm to join Saefwell as CFO in 2019.

Greg was promoted to the position of Saefwell's CEO in 2021.

Bai Jing, Director of Physical Security Services

Bai has a master's degree in human resource management. She has worked as a human resources manager in several large companies. She joined Saefwell as a senior manager in human resources in 2018, with specific responsibility for physical security staff.

Bai was promoted to Saefwell's Board as Director of Physical Security Services in 2022.

Murat Aydin, Director of Intelligence-led Security Services

Murat has a degree in computer science and spent his early career working in systems development for a major bank. He has also served as a computer audit specialist with a major accountancy firm. Murat joined Saefwell in 2016 as a senior consultant in IT security.

Murat was promoted to Saefwell's Board as Director of Intelligence-led Security Services in 2021.

Sabine Anselm, Chief Finance Officer (CFO)

Sabine has a degree in economics and is a qualified accountant. She has worked for several manufacturing companies and spent several years working overseas before returning to Barrland in 2015 to join Saefwell as a senior manager in finance.

Sabine was promoted to CFO in 2022.

John Sokosi, Director of Legal, Risk and Business Ethics

John has a bachelor's degree in law and a master's degree in international law. He is a qualified lawyer. He spent much of his career working for a commercial law firm, before moving to an insurance company as its in-house lawyer. John joined Saefwell's Legal Department in 2019.

John was promoted to Saefwell's Board as Director of Legal, Risk and Business Ethics in 2020.

Professor Martine Anderson, Senior Independent Director

Martine had a successful academic, teaching and researching in international business before being promoted to the position of assistant principal at Central City Technical University. Martine retired from academia in 2020.

Martine joined Saefwell's Board as Senior Independent Director in 2021.

Nils Fall, Independent Non-Executive Director

Nils was a senior actuary with an insurance company, being promoted to assistant director in 2015. He retired from the insurance industry in 2019. He has an active interest in the arts, currently serving as a Board member of Barrland National Opera.

Nils joined Saefwell's Board in 2023.

Magdalena Markowska, Independent Non-Executive Director

Magdalena has worked in procurement for a major car manufacturer. She has held a number of specific roles, including being responsible for the smooth operation of the manufacturer's supply chain. Magdalena retired from full-time employment in 2019. She has since served on the Board of a major international charity.

Magdalena joined Saefwell's Board in 2022.

Board responsibilities

Greg Hainge Chief Executive Officer			
Bai Jing Director of Physical Security Services	Murat Aydin Director of Intelligence-led Security Services	Sabine Anselm Chief Finance Officer (CFO)	John Sokosi Director of Legal, Risk and Business Ethics
<ul style="list-style-type: none"> Business development for physical security clients Human resource management for physical security staff 	<ul style="list-style-type: none"> Business development for intelligence-led security clients Human resource management for intelligence-led security staff 	<ul style="list-style-type: none"> Financial reporting Management accounting Treasury 	<ul style="list-style-type: none"> Health and safety Compliance Enterprise risk management for Saefwell

	Board committees			
	Audit	Risk	Remuneration	Nomination
Dr Pratima Thakali Non-Executive Chair	◆	◆		◆
Professor Martine Anderson Senior Independent Director		◆	◆	◆
Nils Fall Independent Non-Executive Director	◆		◆	◆
Magdalena Markowska Independent Non-Executive Director	◆	◆	◆	

Saefwell's Chief Internal Auditor reports to the convener of the Audit Committee.

Saefwell's Principal Risks

Risk impact	Risk mitigation
<p>Both physical security services and intelligence-led security services rely heavily on Saefwell's ability to recruit and train large numbers of suitable staff. Staffing needs are constantly growing, both in terms of staff numbers and the skills that are required for the increasingly sophisticated assignments that Saefwell agrees to undertake.</p>	<p>Saefwell has strong human resources policies in place to deal with screening new staff to ensure that they have the required skills, experience and character.</p> <p>Saefwell monitors staff turnover closely and is responsive to emerging concerns about staff retention. The firm provides industry-leading training and rewards for staff at all levels.</p>
<p>The nature of physical security and some intelligence-led services expose staff to health and safety risks.</p> <p>Physical security assignments can require staff to work in dangerous environments and may require employees to confront intruders.</p> <p>Consultants on intelligence-led assignments may be exposed to health risks associated with foreign travel. They may also be required to simulate breaches of clients' properties.</p>	<p>All assignments are subject to rigorous risk assessments. Saefwell refuses contracts where the risks are deemed unacceptable.</p> <p>Staff are trained to operate in specific high-risk environments as appropriate to their assignments and are issued with all necessary safety equipment.</p> <p>Consultants are briefed on all risks associated with travel and are provided with all necessary vaccinations. There are strict protocols in place to address risks arising from simulated breaches.</p>
<p>Providing risk management services exposes Saefwell to reputational risk in the event of an alleged failure.</p> <p>The provision of physical security services creates the risk of injury to security staff, client staff and third parties (including bystanders and alleged perpetrators). There is also the risk associated with the loss or destruction of property or premises that are under Saefwell's protection.</p> <p>Intelligence-led security services could leave the company's reputation at risk in the event of allegations that clients were advised poorly or that investigations were conducted and reported in a negligent manner.</p>	<p>Saefwell's risk assessments prior to the acceptance of any assignment take the risk of reputational damage into consideration. Assignments may be refused if the risk of alleged failure is high.</p> <p>Assignments, both physical security and intelligence led, are staffed by suitably trained and experienced guards and consultants. Additional training and equipment are provided where necessary.</p> <p>Consulting teams engaged in intelligence-led security services are well supervised and any reports that are to be presented to clients are reviewed by senior staff before they are submitted.</p>
<p>Saefwell enters into complex, long-term and high-value contracts with clients, particularly in relation to physical security services. Contract terms can prove onerous. For example, foreign contracts may be billed in clients' currencies.</p>	<p>All contracts are subject to detailed review by in-house legal staff. Ongoing contracts are reviewed regularly and any adverse issues are identified and managed where possible.</p>
<p>Saefwell is subject to information security risks. The company holds files relating to the security and strategic management of many large clients.</p>	<p>The company has invested heavily in the latest cyber controls and defences. All risks are monitored on an ongoing basis and mitigated immediately.</p>

Saefwell Group

**Consolidated statement of profit or loss
for the year ended 31 December**

	2023	2022
	B\$ million	B\$ million
Revenue	16,840	15,830
Operating costs	(14,146)	(13,378)
Operating profit	2,694	2,452
Finance costs	(200)	(200)
	2,494	2,252
Tax expense	(399)	(360)
Profit for the year	2,095	1,892

Saefwell Group

**Consolidated statement of changes in equity
for the year ended 31 December 2023**

	Share capital	Retained earnings	Currency reserve	Total
	B\$ million	B\$ million	B\$ million	B\$ million
Opening balance	500	2,667	(360)	2,807
Profit for year		2,095		2,095
Dividend		(1,869)		(1,869)
Loss on translation			(11)	(11)
Closing balance	500	2,893	(371)	3,022

Saefwell Group
Consolidated statement of financial position
as at 31 December

	2023	2022
	B\$ million	B\$ million
Assets		
Non-current assets		
Property, plant and equipment	1,337	998
Goodwill	2,028	2,028
Other intangible assets	1,304	1,388
	<u>4,669</u>	<u>4,414</u>
Current assets		
Trade receivables	1,940	1,898
Bank	1,684	1,572
	<u>3,624</u>	<u>3,470</u>
Total assets	<u><u>8,293</u></u>	<u><u>7,884</u></u>
Equity		
Share capital	500	500
Currency reserve	(371)	(360)
Retained earnings	2,893	2,667
	<u>3,022</u>	<u>2,807</u>
Liabilities		
Non-current liabilities		
Borrowings	2,000	2,000
Current liabilities		
Trade payables	2,870	2,714
Tax liability	401	363
	<u>3,271</u>	<u>3,077</u>
Total equity and liabilities	<u><u>8,293</u></u>	<u><u>7,884</u></u>

Extract from competitor's financial statements

Brotto Security Group is one of four security companies based in Barrland that offers both physical security services and intelligence-led services. Like Saefwell, it focusses on security and does not offer other types of services, such as facilities management. Saefwell and Brotto Security frequently compete for the same assignments.

Brotto Security Group

Consolidated statement of profit or loss for the year ended 31 December

	2023	2022
	B\$ million	B\$ million
Revenue	12,796	12,156
Operating costs	(11,005)	(10,576)
Operating profit	1,791	1,580
Finance costs	(180)	(180)
	1,611	1,400
Tax expense	(258)	(224)
Profit for the year	1,353	1,176

Brotto Security Group

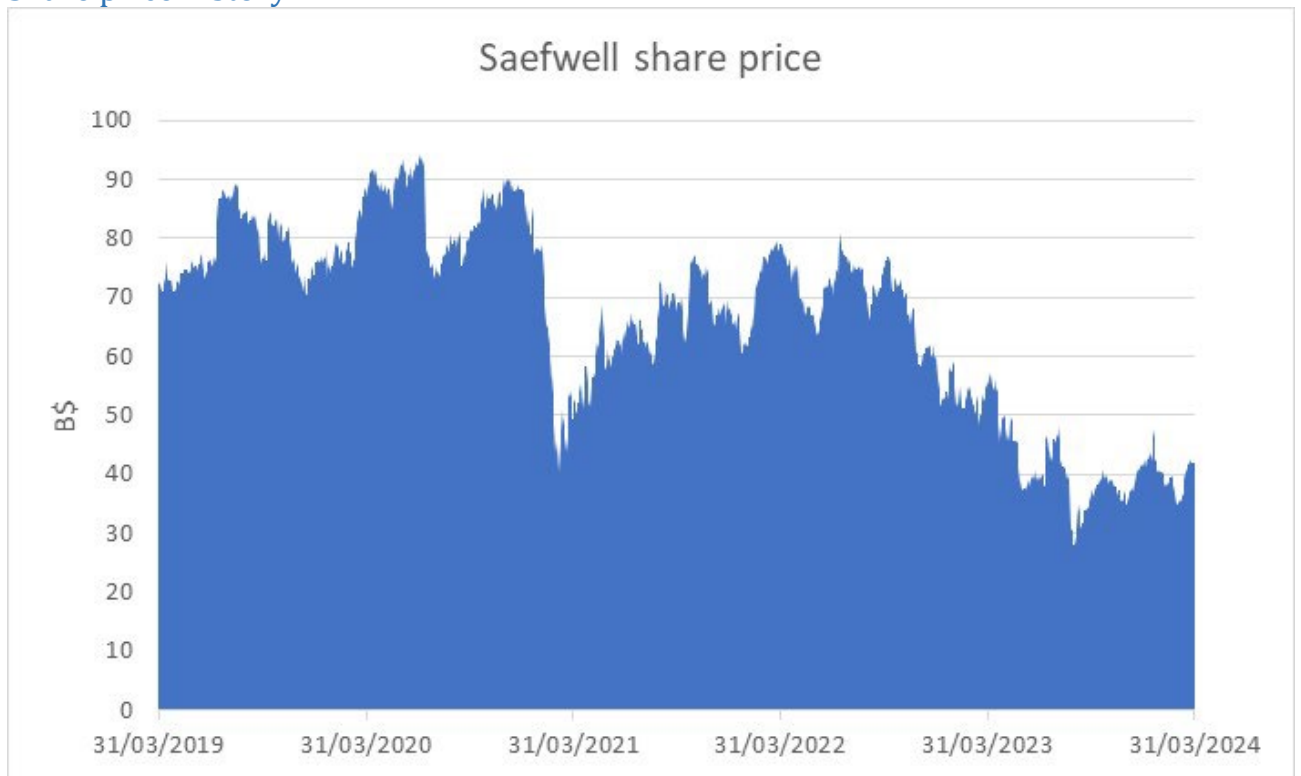
Consolidated statement of changes in equity for the year ended 31 December 2023

	Share capital	Retained earnings	Currency reserve	Total
	B\$ million	B\$ million	B\$ million	B\$ million
Opening balance	450	1,285	(261)	1,474
Profit for year		1,353		1,353
Dividend		(1,169)		(1,169)
Loss on translation			(8)	(8)
Closing balance	450	1,469	(269)	1,650

Brotto Security Group
Consolidated statement of financial position
as at 31 December

	2023	2022
	B\$ million	B\$ million
Assets		
Non-current assets		
Property, plant and equipment	1,248	1,186
Goodwill	1,570	1,570
Other intangible assets	1,271	1,252
	<u>4,089</u>	<u>4,008</u>
Current assets		
Trade receivables	1,474	1,455
Bank	786	664
	<u>2,260</u>	<u>2,119</u>
Total assets	<u><u>6,349</u></u>	<u><u>6,127</u></u>
Equity		
Share capital	450	450
Currency reserve	(269)	(261)
Retained earnings	1,469	1,285
	<u>1,650</u>	<u>1,474</u>
Liabilities		
Non-current liabilities		
Borrowings	1,800	1,800
Current liabilities		
Trade payables	2,640	2,627
Tax liability	259	226
	<u>2,899</u>	<u>2,853</u>
Total equity and liabilities	<u><u>6,349</u></u>	<u><u>6,127</u></u>

Share price history

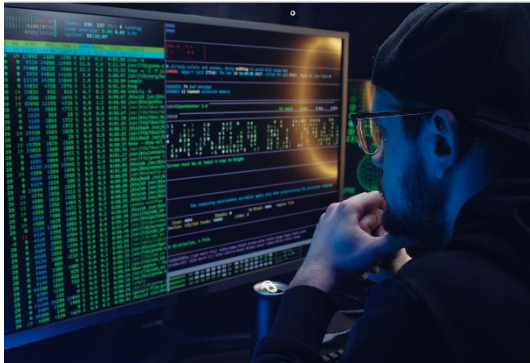


Saefwell's beta is 0.88.

News stories

Barrland Telegraph

New rules require better reporting of digital risks



The Barrlandian Stock Exchange has announced new disclosure rules that will require all companies quoted on the Exchange to include disclosures on digital security and strategy in their annual reports. These new rules are a response to recent scandals involving major corporations who have failed to protect customers' personal data or who have been subject to successful cyber-attacks.

The new legislation will require companies to provide annual disclosures to confirm that they

have adequate strategies in place in relation to digital security. Companies will have to confirm that risks have been assessed and that responsibility for their management has been allocated to appropriate managers.

Companies will also be required to disclose details of events in which attempts were made to breach digital security, regardless of whether those attempts were successful. Those disclosures will indicate whether those events have revealed shortcomings in the company's systems and controls.

A spokesperson for the Barrlandian Stock Exchange commented that these new disclosures will be valuable in informing shareholders about the risks relating to digital security.

The new disclosures will become mandatory for financial years ending on or after 31 December 2025.

Barrland Telegraph

Steady demand for forensic accountants



The word forensic is generally associated with the application of scientific methods to the collection of evidence that can be presented in court. Forensic accounting is a branch of accounting that deals with the collection and presentation of evidence that might be presented in either a civil or criminal case.

Civil cases might involve drafting reports that attach values to claims that may be in dispute. For example, a business could pay a forensic

accountant to estimate the losses attributable to an accident that has interrupted production. That estimate could be used to negotiate compensation with the business's insurer and might be presented in court in the event that a satisfactory agreement cannot be reached.

Criminal cases might require a combination of both accounting skills and the rules of evidence that apply in the criminal courts. For example, if a member of staff is under suspicion of fraud, a forensic accountant might gather evidence by reading the files on the suspect's company laptop. A forensic accountant would have the skills required to examine the laptop in such a way that the suspect cannot complain that files have been altered or that evidence has been fabricated.

Forensic accounting can take many different forms and forensic accountants are always in demand. Most forensic accountants specialise in investigations relating to valuing losses arising from civil cases or gathering evidence for use in criminal cases. One aspect of forensic accounting that is growing in demand is the provision of litigation support, which can involve the use of forensic accountants who specialise in appearing in court as expert witnesses. That may involve giving evidence that clarifies the meaning of reports and investigations to make them clear and understandable to the jury.

Barrland Daily

Bank security guard tackles robbers



A bank security guard was congratulated by senior police officers for his part in apprehending two ruthless bank robbers. The guard was on duty at the entrance to the Glowtown branch of Barrland Prudential Bank when two masked robbers armed with batons pushed past him and demanded that bank staff surrender the cash from their tills.

The security guard activated the bank's alarm and disarmed both robbers, subduing them and tying their wrists together until the police arrived and took charge of the scene. No customers were injured.

The security guard served in the Barrlandian Army, where he was trained in unarmed combat.

A professor of law at Central City University told the Barrland Daily that security guards do not have the same powers of arrest as the police. They are, however, citizens and so are permitted to use "reasonable force" to defend themselves and others from violence and to prevent criminals from escaping. It is highly unlikely that the security guard could be charged with assault in these circumstances, unless the force used to subdue the robbers was deemed excessive.

Barrland Daily

Justice Minister denies that police are underpaid



Barrland's Justice Minister has been criticised for underpaying members of the Police Service. Retention rates are declining across the country, with experienced officers resigning in response to poor pay and stressful work conditions.

The Minister expressed concern that it is difficult for the Police Service to remain competitive with private sector employers. For example, security companies frequently offer higher salaries for shorter working hours. Many police officers find it difficult to resist such opportunities.

Similar concerns have been noted by Barrland's military. Fewer members of the Army, Navy and Air Force are extending their contracts to remain in their chosen services. Again, many are tempted by superior rewards being offered in the private sector.

A government source admitted that the loss of experienced personnel was a problem, particularly when they have specialised skills, such as pilots or medical staff.

Barrland Daily

Take care when installing security cameras



Homeowners have been warned to take care when installing security cameras on their properties. These devices are becoming increasingly popular, being cheap to buy and easy to install. Sensors built into the cameras detect motion and trigger both audio and video recording, with the resulting files being uploaded to the Cloud. These cameras discourage burglars and other intruders, but there are concerns about the legality of their recordings. In some circumstances, homeowners may be breaking strict laws designed to protect privacy and personal data.

Barrland is one of many countries that protects access to individuals' personal data. Legislation makes it a crime to collect data without permission. "Data" includes video footage collected by closed-circuit television (CCTV) systems. The law was intended to regulate the operation of commercial CCTV systems, but it also applies to domestic security cameras.

A lawyer advised the Barrland Daily that homeowners should check the positioning of their cameras. There is unlikely to be a problem if their field of view is restricted to the homeowner's property. The homeowner could be at risk of prosecution if the camera's coverage includes public property or, worse, private property belonging to someone else. Cameras should not, for example, be able to record activity on public pavements or in neighbours' gardens.



Strategic Case Study Exam

Maximum Time Allowed: 3 Hours

Welcome, Candidate Name

If this is not your name, please let your administrator know.


Click **Next** to start the test.

This examination is structured as follows:

Section number	Time for section (minutes)	Number of tasks	Number of sub-task/s	% time to spend on each sub-task
1	60	1	2	(a) 50% (b) 50%
2	60	1	2	(a) 40% (b) 60%
3	60	1	2	(a) 60% (b) 40%

Each section (task) has a number of sub-tasks. An indication of how much of the time available for the section that you should allocate to planning and writing your answer is shown against each sub-task in the text of the question (and summarised in the table above).

This information will be available for you to access during the examination by clicking on the Pre-seen button.

 Reference Material Pre-seen

Sabine Anselm, Chief Finance Officer, stops by your workspace:

"I have brought you an extract from the minutes of this morning's Board meeting. No decision has been taken on whether to accept the assignment from Wavhull.

The Board is meeting tomorrow to discuss the assignment. I need the following from you:

- Firstly, identify and evaluate the implications for the stakeholders of both Saefwell and Wavhull who will be affected if Saefwell accepts this assignment.

[sub-task (a) = 50%]

- Secondly, identify and evaluate the ethical implications for Saefwell of accepting this assignment under the pretence of conducting a risk assessment, as requested by Wavhull's Non-Executive Chair."

[sub-task (b) = 50%]

The extract referred to by Sabine can be viewed by clicking on the Reference Material button above.

Extract from Board minutes










Murat Aydin, Director of Intelligence-led Security Services, requested the Board's advice concerning the acceptance of an assignment to investigate possible bribery by the Chief Executive of Wavhull, a quoted shipbuilder. Wavhull's Non-Executive Chair suspects that her Chief Executive paid B\$8 million to bribe one of the directors of a customer, identified only as "Company X", to award a shipbuilding contract to Wavhull.










Wavhull's Chief Executive issued a verbal instruction to Wavhull's Cashier to pay B\$8 million to "Company Y" for "technical advice". The Cashier made the payment. Wavhull's Non-Executive Chair subsequently investigated Company Y and discovered that it is an unquoted company that is wholly owned by Company X's Director of Shipping. Company X awarded a B\$250 million shipbuilding contract to Wavhull immediately after the B\$8 million payment to Company Y.

Wavhull's Non-Executive Chair strongly suspects that the B\$8 million payment to Company Y was an illegal bribe to Company X's Director of Shipping, intended to ensure that Wavhull was awarded the B\$250 million shipbuilding contract. She wishes Saefwell to investigate whether the B\$8 million payment was a bribe. She wishes Saefwell's investigation to be conducted under the pretence of conducting a risk assessment of negotiating shipbuilding contracts. She has not spoken to anyone else about her suspicions because she does not wish to risk being accused of making false accusations in the event that her suspicions turn out to be false or cannot be proved.

 Reference Material Pre-seen

Draft your response to Sabine's requests in the box below.

       **B** *I* U  x_2 x^2 

Paragraph ▾  ▾        

Reference Material

Pre-seen

A month later, Saefwell has accepted the Wavhull assignment and its investigation into whether Wavhull's Chief Executive bribed one of Company X's directors is under way.

You receive the following email:

From: Sabine Anselm, Chief Finance Officer
To: Senior Finance Manager
Subject: FWD: Wavhull assignment

I have sent you a copy of an email that I received from Saefwell's Director of Intelligence-led Security Services.

I need the following from you:

- Firstly, evaluate the arguments for and against having Saefwell's Internal Audit Department review the work done to date by the consultants before we decide whether to investigate further.
[sub-task (a) = 40%]
- Secondly, evaluate the likely impact on Saefwell's share price if the rumours concerning the true purpose of the Wavhull investigation are reported in the press.
[sub-task (b) = 60%]

Regards

Sabine

The email referred to by Sabine can be viewed by clicking on the Reference Material button above.

From: Murat Aydin, Director of Intelligence-led Security Services

To: Sabine Anselm, Chief Finance Officer

Subject: Wavhull assignment

Hi Sabine,

I have taken a personal interest in the progress of the Wavhull investigation. The facts are as follows:

- Wavhull's Non-Executive Chair believes that the company's Chief Executive bribed the Director of Shipping at Company X with a payment of B\$8 million in return for the award of a B\$250 million shipbuilding contract to Wavhull. She believes that the bribe was paid indirectly through Company Y, which is wholly owned by Company X's Director of Shipping.
- Wavhull's Chief Executive gave Wavhull's Cashier a verbal instruction to pay B\$8 million to Company Y for "technical advice". The Cashier regarded this instruction as irregular and sent an email saying so to both the Chief Executive and the Non-Executive Chair before making the payment. The Cashier received an acknowledgement of the email from the Non-Executive Chair but received no response from the Chief Executive.
- Wavhull's Head of Design confirms that Company Y supplied Wavhull with some engineering documents. The Head of Design had not requested these and did not find them particularly useful.
- Saefwell's consultants have investigated the relationship between Company X and Company Y and have confirmed that Company Y is wholly owned by Company X's Director of Shipping. They have found no other connection between Company X and Company Y.

Saefwell's consultants have told Wavhull's managers and staff that they are conducting a risk assessment on the negotiation of shipbuilding contracts. However, rumours are beginning to circulate that the integrity of Wavhull's directors is being investigated. Wavhull is a quoted company.

The senior consultant in charge of Saefwell's investigation does not believe that it will be possible to gather convincing evidence concerning the bribery allegations without first interviewing Wavhull's Chief Executive and asking him to prove that the B\$8 million payment was justified. That will, of course, require the Non-Executive Chair's permission. I wonder whether it would be helpful to have Saefwell's Internal Audit Department review the work done to date by Saefwell's consultants before we decide whether to proceed further with this investigation.

Regards

Murat

 Reference Material Pre-seen



Draft your response to Sabine's requests in the box below.

From: Senior Finance Manager

To: Sabine Anselm, Chief Finance Officer

Subject: FWD: RE: Wavhull assignment



 Reference Material Pre-seen

Three months later, the Wavhull investigation has concluded. Saefwell's consultants were unable to decide whether the evidence that has been gathered is sufficient to have Wavhull's Chief Executive prosecuted for bribery.

You receive the following email:

From: Sabine Anselm, Chief Finance Officer
To: Senior Finance Manager
Subject: FWD: Potential acquisition

Hello,

I have forwarded an email that I received from Greg Hainge, Saefwell's Chief Executive Officer.

I need your advice on two matters:

- Firstly, evaluate the arguments for and against Greg's belief that the acquisition of Laubooker would benefit the Saefwell Group.
[sub-task (a) = 60%]
- Secondly, identify and evaluate the post-acquisition issues that might have a negative impact on Saefwell's acquisition of Laubooker.
[sub-task (b) = 40%]

Regards

Sabine

The email referred to by Sabine can be viewed by clicking on the Reference Material button above.

From: Greg Hainge, Chief Executive Officer
To: Sabine Anselm, Chief Finance Officer
Subject: Potential acquisition

Hi Sabine,

I am concerned that our consultants were unable to offer a clear recommendation as to whether we had established a strong legal case against Wavhull's Chief Executive. We took legal advice, but that was also unclear. This is not the first time that an important assignment has not reached a satisfactory conclusion because of concerns about taking a case to court.



I might have found the answer to this problem. Laubooker is a forensic accounting firm that specialises in litigation support. It employs 120 professional staff, most of whom are qualified as both accountants and lawyers. One of their senior consultants reviewed our Wavhull files and provided me with a clear opinion that we had insufficient evidence against the Chief Executive. She recommended some additional work that would clarify our position.

Laubooker is an unquoted company. It was founded 10 years ago by four forensic accountants who had also had legal training. The founders continue to serve as directors. The directors are keen for Laubooker to maintain a low profile and avoid publicity.

I believe that we could acquire Laubooker as a 60% subsidiary, with its founders retaining the remaining 40%.

Regards

Greg

 Reference Material Pre-seen

Draft your response to Sabine's requests in the box below.

From: Senior Finance Manager

To: Sabine Anselm, Chief Finance Officer

Subject: FWD: RE: Potential acquisition



A large, empty rectangular box for drafting the response to Sabine's requests.



Thank you for completing the Strategic Case Study Exam.

Before you leave, don't forget to collect your printed confirmation of attendance.

Please click the End Exam (E) button before leaving the testing room quietly.



Strategic Case Study Exam

Maximum Time Allowed: 3 Hours

Welcome, Candidate Name

If this is not your name, please let your administrator know.



Click **Next** to start the test.

This examination is structured as follows:

Section number	Time for section (minutes)	Number of tasks	Number of sub-task/s	% time to spend on each sub-task
1	60	1	2	(a) 50% (b) 50%
2	60	1	2	(a) 60% (b) 40%
3	60	1	2	(a) 40% (b) 60%

Each section (task) has a number of sub-tasks. An indication of how much of the time available for the section that you should allocate to planning and writing your answer is shown against each sub-task in the text of the question (and summarised in the table above).

This information will be available for you to access during the examination by clicking on the Pre-seen button.

 Reference Material Pre-seen

Sabine Anselm, Chief Finance Officer, invites you into her office:

"This news article has just gone online. Saefwell has not yet had to publish an annual report since the new rules relating to digital security were announced.

I need your advice on two matters before I brief the rest of the Board.

- Firstly, discuss the implications of the share price movements described in the final paragraph of the news article for quoted companies that must decide whether or not to make voluntary disclosures on digital security in their annual reports.

[sub-task (a) = 50%]

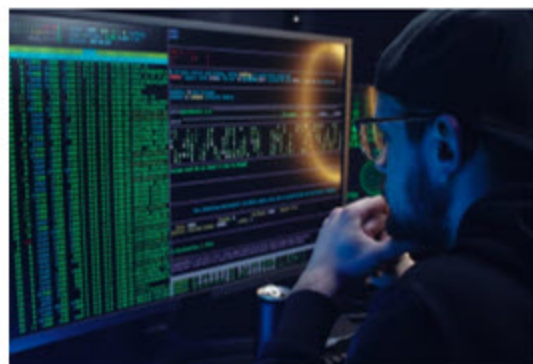
- Secondly, identify and evaluate the governance issues for Saefwell that are associated with managing digital security risks and recommend with reasons how Saefwell might manage those issues."

[sub-task (b) = 50%]

The news article referred to by Sabine can be viewed by clicking on the Reference Material button above.

Barrland Telegraph



New disclosures on digital security start to take effect












The Barrlandian Stock Exchange recently announced strict new disclosure requirements concerning digital security. Once the rules come into effect, companies will be required to disclose information relating to digital security, including details of events in which attempts have been made to breach data security, whether those attempts were successful and whether existing strategies were sufficient to handle the attempt.










These disclosures will not become mandatory until financial years ending on or after 31 December 2025, but companies are permitted to comply sooner if they wish to do so. Roughly half of the companies who have published annual reports since the rules were issued have made the disclosures voluntarily.

Analysts have studied the impact of voluntary disclosures on share prices, adjusting to exclude the effects of other variables. The companies who made voluntary disclosures have tended to suffer small decreases in share prices. Companies who have chosen not to disclose have tended to suffer larger decreases in their share prices.

 Reference Material Pre-seen

Draft your response to Sabine's requests in the box below.

       **B** *I* U  x_2 x^2 

Paragraph ▾  ▾        

 Reference Material Pre-seen

A month later, you receive the following email:

From: Sabine Anselm, Chief Finance Officer
To: Senior Finance Manager
Subject: Potential acquisition

Hello,

I have attached an extract from the minutes of this morning's Board meeting.

I need your help with two matters:

- Firstly, evaluate the opportunities and threats to the Saefwell Group arising from the new disclosures of digital security risks, assuming that we acquire Inbyte to assist with the increased demand for professional services.

[sub-task (a) = 60%]

- Secondly, recommend with reasons the approach that Saefwell should take to the evaluation and management of the currency risks arising from ownership of Inbyte.

[sub-task (b) = 40%]

Regards

Sabine

The extract referred to by Sabine can be viewed by clicking on the Reference Material button above.

Extract from Board minutes**Potential acquisition**

Murat Aydin, Director of Intelligence-led Security Services, informed the Board that the new reporting requirements in respect of digital security are expected to have a significant impact on Barrlandian quoted companies. The rules require disclosure of events such as attempted breaches. Companies are required to disclose whether their digital security strategies were sufficient to deal with attempted breaches. Stakeholders are paying close attention to these new disclosures because they are forcing companies to provide far more information about cyber risks than was previously the case. Saefwell has been asked to advise many existing and new clients about the new disclosure rules.

Mr Aydin informed the Board that he had held informal talks with the directors of Irnbyte, an unquoted digital security company based in Renoland. Irnbyte employs 1,200 consultants who specialise in the evaluation of digital security systems and in recommending responses to weaknesses. These consultants can operate remotely and so could support clients based in Barrland without having to relocate. Saefwell could use Irnbyte's consultants to service clients and could invoice in B\$. Irnbyte's directors hold 100% of the company's shares. They would be willing to sell their company to Saefwell in return for a cash payment.

Renoland has a weaker economy than Barrland, where Saefwell is based, but educational standards are high and the country has a strong reputation for the development of information systems. There is a volatile exchange rate between Renoland's currency, the R\$, and the B\$, Saefwell's home currency.

The Board agreed to consider the proposal to acquire Irnbyte.

 Reference Material Pre-seen

Draft your response to Sabine's requests in the box below.



From: Senior Finance Manager

To: Sabine Anselm, Chief Finance Officer

Subject: RE: Potential acquisition



A large, empty text area for drafting the response to Sabine's requests.

 Reference Material Pre-seen

The following day, you receive the following email:

From: Sabine Anselm, Chief Finance Officer
To: Senior Finance Manager
Subject: FWD: Digital security disclosures

Hello,

I have forwarded an email from John Sokosi, Director of Legal, Risk and Business Ethics.

I need your advice on two matters:

- Firstly, recommend with reasons the manner in which quoted companies might report their performance in order to reassure stakeholders that they are committed to the proper management of digital security.

[sub-task (a) = 40%]

- Secondly, evaluate the ethical arguments for and against omitting "trivial" incidents from the report on digital security.

[sub-task (b) = 60%]

Regards

Sabine

The email referred to by Sabine can be viewed by clicking on the Reference Material button above.

From: John Sokosi, Director of Legal, Risk and Business Ethics

To: Sabine Anselm, Chief Finance Officer

Subject: Digital security disclosures

Hello Sabine,

Saefwell has been receiving large numbers of queries from clients concerning the implications of the new Stock Exchange requirement that requires quoted companies to report on their strategies for managing digital risks. Clients are also raising queries concerning the requirement to report on the number of attempts to breach their systems and the extent to which their strategies were able to withstand those attempts.



Many of the queries that we have received relate to the way in which boards can demonstrate their commitment to setting effective digital security strategies. The directors of many of our clients wish to know how they might be able to reassure shareholders and other stakeholders that they take digital security seriously.

We also receive queries about the need to report every "incident" involving attempted breaches of clients' systems. Many of our clients have pointed out that some incidents are too trivial to report and that reporting them would be misleading. For example, if a customer mistypes a username or password when trying to log into an online account, that could be classified as an attempt to gain unauthorised access.

I intend to have my staff draft some guidance that can be issued to clients.

Regards

John

 Reference Material Pre-seen

Draft your response to Sabine's requests in the box below.

From: Senior Finance Manager

To: Sabine Anselm, Chief Finance Officer

Subject: FWD: RE: Digital security disclosures



A large, empty rectangular box for drafting the response to Sabine's requests.



Thank you for completing the Strategic Case Study Exam.

Before you leave, don't forget to collect your printed confirmation of attendance.

Please click the End Exam (E) button before leaving the testing room quietly.



Strategic Case Study Exam

Maximum Time Allowed: 3 Hours

Welcome, Candidate Name

If this is not your name, please let your administrator know.

Click **Next** to start the test.

This examination is structured as follows:

Section number	Time for section (minutes)	Number of tasks	Number of sub-task/s	% time to spend on each sub-task
1	60	1	2	(a) 50% (b) 50%
2	60	1	2	(a) 60% (b) 40%
3	60	1	2	(a) 40% (b) 60%

Each section (task) has a number of sub-tasks. An indication of how much of the time available for the section that you should allocate to planning and writing your answer is shown against each sub-task in the text of the question (and summarised in the table above).

This information will be available for you to access during the examination by clicking on the Pre-seen button.

Reference Material

Pre-seen

You have received the following email:

From: Sabine Anselm, Chief Finance Officer
To: Senior Finance Manager
Subject: Neerland subsidiary

Hello,

I have attached a news report that has just gone online. Neerland is a developed country. We have many clients there, who provide a total of 7% of the Saefwell Group's revenue.

Saefwell has a global strategy of using security cameras to cover access points to clients' premises. Cameras are a cost-effective deterrent that reduces the number of security guards required to protect any given location. We do often position cameras to look beyond client property, which is technically against the law in most countries.

The wider coverage significantly enhances security.

I need your advice on two matters:

- Firstly, evaluate the political risks that these concerns about security cameras might create for Saefwell in relation to its operations in Neerland.

[sub-task (a) = 50%]

- Secondly, recommend with reasons whether Saefwell should adopt an emergent approach to the development of strategies for providing clients with physical security services.

[sub-task (b) = 50%]

Regards

Reference Material

Pre-seen

You have received the following email:

From: Sabine Anselm, Chief Finance Officer
To: Senior Finance Manager
Subject: Neerland subsidiary

Hello,

I have attached a news report that has just gone online. Neerland is a developed country. We have many clients there, who provide a total of 7% of the Saefwell Group's revenue.

Saefwell has a global strategy of using security cameras to cover access points to clients' premises. Cameras are a cost-effective deterrent that reduces the number of security guards required to protect any given location. We do often position cameras to look beyond client property, which is technically against the law in most countries.

The wider coverage significantly enhances security.

I need your advice on two matters:

- Firstly, evaluate the political risks that these concerns about security cameras might create for Saefwell in relation to its operations in Neerland.

[sub-task (a) = 50%]

- Secondly, recommend with reasons whether Saefwell should adopt an emergent approach to the development of strategies for providing clients with physical security services.

[sub-task (b) = 50%]

Regards

Reference Material

Pre-seen

You have received the following email:

From: Sabine Anselm, Chief Finance Officer

To: Senior Finance Manager

Subject: Neerland subsidiary

Hello,

I have attached a news report that has just gone online. Neerland is a developed country. We have many clients there, who provide a total of 7% of the Saefwell Group's revenue.

Saefwell has a global strategy of using security cameras to cover access points to clients' premises. Cameras are a cost-effective deterrent that reduces the number of security guards required to protect any given location. We do often position cameras to look beyond client property, which is technically against the law in most countries.

The wider coverage significantly enhances security.

I need your advice on two matters:

- Firstly, evaluate the political risks that these concerns about security cameras might create for Saefwell in relation to its operations in Neerland.

[sub-task (a) = 50%]

- Secondly, recommend with reasons whether Saefwell should adopt an emergent approach to the development of strategies for providing clients with physical security services.

[sub-task (b) = 50%]

Regards

Sabine

The news report referred to by Sabine can be viewed by clicking on the Reference Material button above.

Barrland Telegraph

Saefwell subsidiary in legal difficulties in Neerland



Neerland's Justice Minister has criticised Saefwell's Neerlandian subsidiary for being in breach of the country's strict data protection and privacy laws.



Neerland's Data Protection Office discovered a problem when its investigators responded to a complaint from a member of the public, who suspected that security cameras operated by Saefwell were recording pedestrians in the street. It was discovered that cameras installed at a client's premises were taking high-definition video of the

street in front of the client's property. It is an offence in Neerland to photograph individuals when they are in a public place unless they have given their permission.

A spokesperson for Saefwell commented that its security cameras frequently view public spaces outside of client premises in order to deter and to detect intruders. These cameras enable the company to secure entrances to clients' property without putting staff employed by the client or by Saefwell at risk.

Neerland's Justice Minister rejected this argument, warning foreign security companies operating in Neerland that they had to respect the country's laws.

Neerland's data protection laws are very similar to Barrland's and, indeed, to those of most countries.

 Reference Material Pre-seen

Draft your response to Sabine's requests in the box below.

From: Senior Finance Manager

To: Sabine Anselm, Chief Finance Officer

Subject: RE: Neerland subsidiary



 Reference Material Pre-seen

The following day, Sabine Anselm asks you to join her in her office:

"I have brought you an extract from this morning's Board meeting.

I need to meet with Greg Hainge later today. I need your advice concerning two matters:

- Firstly, evaluate whether the significant decrease in Saefwell's share price is inconsistent with both:
 - the fact that the company has not announced its intentions with respect to its widespread use of security cameras
 - the company's low beta coefficient.

[sub-task (a) = 60%]

- Secondly, evaluate the argument that Saefwell's directors should have foreseen the negative publicity relating to the manner in which it uses security cameras."

[sub-task (b) = 40%]



The extract referred to by Sabine can be viewed by clicking on the Reference Material button above.

Extract from Board minutes**Security cameras**















Greg Hainge, Chief Executive Officer, reminded the Board that Saefwell had suffered some negative publicity over the manner in which it uses security cameras in Neerland. 7% of the Saefwell Group's revenue is earned in that country.

Bai Jing, Director of Physical Security Services, informed the Board that Saefwell does not comply with data protection laws in many of the countries in which it operates, not just in Neerland. Saefwell will have to reduce its reliance on security cameras if it is to become compliant.

Sabine Anselm, Chief Finance Officer, informed the Board that Saefwell's share price had decreased by 8% since news of the events in Neerland. The Board expressed surprise concerning this drop. It was pointed out that Saefwell has not released any information about its intended response to the complaints relating to data protection. Also, Saefwell's beta coefficient is less than 1.0.





















 Reference Material Pre-seen



Draft your response to Sabine's requests in the box below.



Paragraph ▾

--	--	--	--	--



 Reference Material Pre-seen

A month later, you receive the following email:

From: Sabine Anselm, Chief Finance Officer
To: Senior Finance Manager
Subject: FWD: Reduction in security cameras

Hello,

I have forwarded an email from Bai Jing, Saefwell's Director of Physical Security Services.

I need your advice on two matters:

- Firstly, evaluate the ethical issues arising from Bai Jing's argument that Saefwell should continue to use security cameras as before, despite the fact that it is in breach of local laws in some cases.

[sub-task (a) = 40%]

- Secondly, recommend with reasons how Saefwell's Internal Audit Department might ensure that staff training and new procedures will be effective in ensuring that security staff assigned to vulnerable access points are safe.

[sub-task (b) = 60%]

Regards

Sabine

The email referred to by Sabine can be viewed by clicking on the Reference Material button above.

From: Bai Jing, Director of Physical Security Services

To: Sabine Anselm, Chief Finance Officer

Subject: Reduction in security cameras

Hello Sabine,

I have decided to review the security arrangements at all of the sites at which we provide security. The objective of this review is to remove all security cameras that are putting us in breach of local data protection laws by filming public spaces, such as pavements in front of clients' access points. We will then have to replace those cameras with alternative security measures, such as stationing security guards to protect vulnerable access points. The cameras that cover the street leading up to an entrance are often the most important of all.

I have already received some negative feedback from managers and supervisors at all levels throughout Physical Security Services. The staff who will be standing guard will be in some danger because they will have to confront intruders directly. We plan to deal with that through staff training and establishing procedures that will ensure that our security guards support one another in the event of any incidents.

I am unhappy that we are being forced to remove these cameras and we might retain some at particularly sensitive locations. We have only received one complaint even though, technically, we have been in breach of the law for several years. None of the video files on our systems have been abused in any way.

Regards

Bai

 Reference Material Pre-seen

Draft your response to Sabine's requests in the box below.

From: Senior Finance Manager

To: Sabine Anselm, Chief Finance Officer

Subject: FWD: RE: Reduction in security cameras



A large, empty rectangular box for drafting the response to Sabine's requests.



Thank you for completing the Strategic Case Study Exam.

Before you leave, don't forget to collect your printed confirmation of attendance.

Please click the End Exam (E) button before leaving the testing room quietly.



Strategic Case Study Exam

Maximum Time Allowed: 3 Hours

Welcome, Candidate Name

If this is not your name, please let your administrator know.



Click **Next** to start the test.

This examination is structured as follows:

Section number	Time for section (minutes)	Number of tasks	Number of sub-task/s	% time to spend on each sub-task
1	60	1	2	(a) 60% (b) 40%
2	60	1	2	(a) 40% (b) 60%
3	60	1	2	(a) 50% (b) 50%

Each section (task) has a number of sub-tasks. An indication of how much of the time available for the section that you should allocate to planning and writing your answer is shown against each sub-task in the text of the question (and summarised in the table above).

This information will be available for you to access during the examination by clicking on the Pre-seen button.

 Reference Material Pre-seen

Sabine Anselm, Chief Finance Officer, stops by your workspace:

"I have brought an extract from a report that has been circulated to the Board. The Head of Internal Security reports to John Sokosi, Director of Legal, Risk and Business Ethics.

I need your advice on two matters before the Board meets to discuss this report:

- Firstly, evaluate the arguments for and against treating Saefwell's cyber security as a strategic matter that should be managed by the Board.

[sub-task (a) = 60%]

- Secondly, recommend with reasons the key performance indicators (KPIs) that the Internal Security Department might submit to the Board."

[sub-task (b) = 40%]

The extract referred to by Sabine can be viewed by clicking on the Reference Material button above.

Attempts to breach Saefwell's corporate security**Executive summary**

Prepared by Yi-Ling Chiang, Head of Internal Security

The Internal Security Department is responsible for all aspects of preventing unauthorised access to Saefwell's assets, both physical and electronic. Our responsibilities include tracking attempts to breach the security of Saefwell's network.










According to our records relating to the year ended 30 June 2024:










- The number of suspicious calls and emails reported to Internal Security by other departments has increased by 60% in comparison to the previous year. Most of these attempted to obtain staff usernames and passwords and were classified as social engineering by the Internal Security Department.
- Incidents notified by Saefwell's security software have increased by 55% compared to the previous year. These included attempts to log into the company's systems using a variety of different electronic techniques.



These increases are significantly higher than those reported by other quoted companies in Barrland. It may be that Saefwell is regarded as an attractive target by potential intruders because its files include details of clients' security systems.

 Reference Material Pre-seen

Draft your response to Sabine's requests in the box below.

       **B** *I* U  x_2 x^2 

Paragraph ▾  ▾        

 Reference Material Pre-seen

A month later, you receive the following email:

From: Sabine Anselm, Chief Finance Officer
To: Senior Finance Manager
Subject: Alleged security breach

Hello,

I have attached a news report that was posted online a few hours ago.

I need your advice on two matters:

- Firstly, identify and evaluate the power and interest of key stakeholder groups (other than shareholders) who are affected by this news report and the actions that Saefwell might take to manage its relationship with those stakeholders.

[sub-task (a) = 40%]

- Secondly, recommend with reasons the actions that Saefwell's Board should take in order to protect the company's share price.

[sub-task (b) = 60%]

Regards

Sabine

The news report referred to by Sabine can be viewed by clicking on the Reference Material button above.

Barrland Daily


Hacker claims to have breached security company's security



An anonymous hacker claims to have accessed confidential files belonging to Saefwell, one of the world's largest security companies. The hacker contacted the Barrland Daily's Chief Business Reporter, attaching copies of files that appear to contain details of the security arrangements at several major companies, all of whom are known to employ Saefwell.

The Barrland Daily has alerted the Police Service's Cybercrimes Unit and will cooperate fully in any criminal investigations into this incident.

A spokesperson for Saefwell commented that it would not be appropriate to comment on the hacker's claims until the company had carried out its own investigation. The spokesperson refused to confirm or deny whether the files were genuine.

 Reference Material Pre-seen



Draft your response to Sabine's requests in the box below.

From: Senior Finance Manager

To: Sabine Anselm, Chief Finance Officer

Subject: RE: Alleged security breach



 Reference Material Pre-seen

Eight months later, you receive the following email:

From: Sabine Anselm, Chief Finance Officer
To: Senior Finance Manager
Subject: Acquisition of security consultancy

Hello,

I have attached an extract from the minutes of this morning's Board meeting concerning Saefwell's recent acquisition of Mowrtron Consulting ('Mowrtron').

I need your advice on two matters:

- Firstly, evaluate the argument that Saefwell's Board should have managed the acquisition of Mowrtron differently. **[sub-task (a) = 50%]**
- Secondly, evaluate the ethical implications of Saefwell's Board remaining silent about the loss of consultants from Mowrtron. **[sub-task (b) = 50%]**

Regards

Sabine

The extract referred to by Sabine can be viewed by clicking on the Reference Material button above.

**Extract from Board minutes****Acquisition of Mowrtron Consulting**

Greg Hainge, Chief Executive Officer, informed the Board that Saefwell had acquired 100% of the equity of Mowrtron Consulting ('Mowrtron'). Mowrtron is a leading cyber security company. The company has developed its own security software, which is adapted by its consultants to meet the needs of individual clients. Saefwell's Board intends to initially use this software to protect Saefwell's network against intruders. However, the software will be made available for sale to clients in the future.

Ramesh Kumar, Mowrtron's founder, sole shareholder and Chief Executive, stepped down as soon as the acquisition was completed.

Mowrtron employed 100 consultants before the acquisition. Saefwell's plan was to retain those consultants for at least 6 months. It was intended that the consultants would install Mowrtron's software on Saefwell's network and also complete work contracted by Mowrtron while it was an independent entity. Saefwell intended to make 50 of Mowrtron's consultants redundant after that initial period, keeping the remainder to ensure that the software protecting Saefwell's network was kept up to date.

70 of Mowrtron's most experienced consultants resigned within 24 hours of the acquisition, with more expected to follow. Rumours of redundancies started to circulate after Mowrtron's staff were informed of the acquisition by an email that made no mention of plans for staffing.

The business press paid very little attention to Saefwell's acquisition of Mowrtron. It is unlikely that the resignations will be regarded as newsworthy.

 Reference Material Pre-seen

Draft your response to Sabine's requests in the box below.

From: Senior Finance Manager

To: Sabine Anselm, Chief Finance Officer

Subject: RE: Acquisition of security consultancy



Large empty text area for drafting the response.



Thank you for completing the Strategic Case Study Exam.

Before you leave, don't forget to collect your printed confirmation of attendance.

Please click the End Exam (E) button before leaving the testing room quietly.



Strategic Case Study Exam

Maximum Time Allowed: 3 Hours

Welcome, Candidate Name

If this is not your name, please let your administrator know.



Click **Next** to start the test.

This examination is structured as follows:

Section number	Time for section (minutes)	Number of tasks	Number of sub-task/s	% time to spend on each sub-task
1	60	1	2	(a) 60% (b) 40%
2	60	1	2	(a) 40% (b) 60%
3	60	1	2	(a) 50% (b) 50%

Each section (task) has a number of sub-tasks. An indication of how much of the time available for the section that you should allocate to planning and writing your answer is shown against each sub-task in the text of the question (and summarised in the table above).

This information will be available for you to access during the examination by clicking on the Pre-seen button.

 Reference Material Pre-seen

You have received the following email:

From: Sabine Anselm, Chief Finance Officer
To: Senior Finance Manager
Subject: Recruitment of cyber security consultants

Hello,

I have attached a news report that has just gone online.

This report is a matter of some concern for Saefwell because we recruit many of our cyber security consultants from the police and military, both in Barrland and in the other countries in which we do business.

I need your help with the following:

- Firstly, using scenario planning thinking, discuss how each of the following possibilities associated with our employment of cyber security experts from the police and military might apply to Saefwell:
 - Barrland's Police Service might match the salaries that security companies, including Saefwell, offer these experts.
 - Barrland's military might offer cyber warfare experts the opportunity to study for a one-year, full-time master's degree in computer science in return for agreeing to enlist for 10 years. Most members of the military enlist for 5 years.
 - The Barrlandian Government might pass legislation that forbids security companies from recruiting cyber security experts currently employed by the Barrlandian police and military.

[sub-task (a) = 60%]

- Secondly, evaluate the political risks associated with doing business in countries from which we recruit cyber security experts from their police and military.

[sub-task (b) = 40%]

Regards

Sabine

The news report referred to by Sabine can be viewed by clicking on the Reference Material button above.

Barrland Telegraph


Ministers battle against poaching of cyber security specialists



The Barrlandian Government has announced plans to reduce the rate at which intelligence officers with expertise in cyber security are being recruited by private sector security companies. This follows similar announcements that the governments of Eastland and Southland were considering similar plans.

Both the military and police find it increasingly difficult to retain staff who serve in specialist units that fight cyber warfare and cyber crime. Soldiers and police officers from such backgrounds are in constant demand for the private sector, where they can earn significantly more because of their training and experience.

The security industry has also been criticised by other countries, whose military and police services face the same difficulties in retaining cyber security specialists.

 Reference Material Pre-seen



Draft your response to Sabine's requests in the box below.

From: Senior Finance Manager

To: Sabine Anselm, Chief Finance Officer

Subject: RE: Recruitment of cyber security consultants



 Reference Material Pre-seen

A month later, you receive the following email:

From: Sabine Anselm, Chief Finance Officer
To: Senior Finance Manager
Subject: FWD: Expanding into public sector

Hello,

I have copied an email from Murat Aydin, Saefwell's Director of Intelligence-led Security Services.

I believe that the only way to finance Murat's proposal would be to suspend the payment of this year's dividend.

I need your advice on two matters:

- Firstly, identify and evaluate the power and interest of two key stakeholder groups (other than shareholders) who would be affected if Saefwell implemented Murat's proposal to offer cyber security services to Barrland's Police Service and recommend with reasons how those stakeholders' interests should be managed.

[sub-task (a) = 40%]

- Secondly, identify and evaluate the implications of suspending Saefwell's dividend in order to finance this new venture.

[sub-task (b) = 60%]

Regards

Sabine

The email referred to by Sabine can be viewed by clicking on the Reference Material button above.

From: Murat Aydin, Director of Intelligence-led Security Services

To: Sabine Anselm, Chief Finance Officer

Subject: Expanding into public sector


Hello Sabine,

I believe that there is an opportunity for Saefwell to offer cyber security services to Barrland's Police Service. The Police Service already makes use of commercial organisations to assist it in key support roles. For example, it has outsourced laboratory analysis of evidence from criminal investigations to a technical support company. In principle, we could undertake most of the routine cyber security work that would be required by the Police, such as protecting communications networks from security breaches. That would leave the Police Service's cyber crimes specialists free to concentrate on investigating cyber crimes and identifying criminals.

Providing this service will require Saefwell to make a significant investment in the recruitment of suitable consultants, their training and in equipping them with suitable hardware and software.

Regards

Murat

 Reference Material Pre-seen



Draft your response to Sabine's requests in the box below.

From: Senior Finance Manager

To: Sabine Anselm, Chief Finance Officer

Subject: FWD: RE: Expanding into public sector



 Reference Material Pre-seen

Six months later, Saefwell has signed a contract to provide cyber security services for the Barrlandian Police Service.

Sabine Anselm asks you to join her in her office:

"I have brought you an extract from the minutes of this morning's Board meeting.

I need your advice on two matters:

- Firstly, recommend with reasons controls that might prevent a recurrence of these errors when checking candidates' backgrounds.
[sub-task (a) = 50%]
- Secondly, evaluate the arguments for and against having Saefwell's Internal Audit Department perform background checks on candidates who are being considered for employment on the Police Service contract."
[sub-task (b) = 50%]

The extract referred to by Sabine can be viewed by clicking on the Reference Material button above.

Extract from Board minutes
Failed recruitment processes

Murat Aydin, Director of Intelligence-led Security Services, informed the Board that recruitment and training of consultants to provide cyber security support for Barrland's Police Service was underway. Saefwell had recruited 200 consultants for this role and applications were still being processed to fill further vacancies.

Unfortunately, a problem has arisen with regard to recruitment. The Police Service carried out its own background checks before permitting newly-recruited consultants access to its systems. A total of 14 consultants failed the Police Service checks, despite having been declared acceptable by Saefwell:










- 7 falsely claimed to have degrees in computer science
- 4 falsely claimed to have had experience in computer security
- 3 falsely claimed to have clean criminal records.










The Police Service is threatening to terminate Saefwell's contract unless there is an improvement in the company's checks on staff who will be involved in this contract.

Mr Aydin pointed out that the applicants' applications had been checked. Those who had lied about qualifications or experience had submitted forged documents in support of their claims. Saefwell's application forms ask candidates to disclose any criminal convictions, but the company cannot access Police files to verify responses.

 Reference Material Pre-seen

Draft your response to Sabine's requests in the box below.

       **B** *I* U  x_2 x^2 

Paragraph ▾  ▾        



Thank you for completing the Strategic Case Study Exam.

Before you leave, don't forget to collect your printed confirmation of attendance.

Please click the End Exam (E) button before leaving the testing room quietly.



Strategic Case Study Exam

Maximum Time Allowed: 3 Hours

Welcome, Candidate Name

If this is not your name, please let your administrator know.



Click **Next** to start the test.

This examination is structured as follows:

Section number	Time for section (minutes)	Number of tasks	Number of sub-task/s	% time to spend on each sub-task
1	60	1	2	(a) 60% (b) 40%
2	60	1	2	(a) 50% (b) 50%
3	60	1	2	(a) 40% (b) 60%

Each section (task) has a number of sub-tasks. An indication of how much of the time available for the section that you should allocate to planning and writing your answer is shown against each sub-task in the text of the question (and summarised in the table above).

This information will be available for you to access during the examination by clicking on the Pre-seen button.

 Reference Material Pre-seen

Sabine Anselm, Chief Finance Officer, asks you to join her in a meeting room:

"I have brought you a newspaper article that has interested members of Saefwell's Board. The physical security services provided by major security companies, including Saefwell, do not offer this type of active penetration testing. To the best of our knowledge, Sneektheef is the only security company that offers this service. Bai Jing, our Director of Physical Security Services, has suggested that we should enter this market.

I plan to brief the Board soon and I need your advice on two matters:

- Firstly, evaluate Bai Jing's proposal in terms of the suitability, feasibility and acceptability (SAF) criteria.

[sub-task (a) = 60%]

- Secondly, identify and evaluate the risks that this type of physical penetration testing could create for Saefwell's consultants."

[sub-task (b) = 40%]

The newspaper article referred to by Sabine can be viewed by clicking on the Reference Material button above.

Barrland Daily

My working day – Barry Thomson



I work for a small security company that specialises in testing clients' physical security systems by attempting to bypass them using the same deception techniques that criminals would use. We call this "penetration testing". If we succeed, then clients know that their systems are vulnerable.










I spent the whole of last week observing a client's reception area from a coffee shop across the street. I quickly realised that one of the security guards was always bored and was paying little attention to his duties. I struck one lunchtime when that guard was alone in reception. I was carrying a cheap rug and told him that I had to deliver it to the boardroom. He gave me a visitor's pass and let me take the lift to the top floor. I abandoned the rug in a cleaning cupboard and was able to access three directors' offices, including the Chief Executive's. I took photographs of the confidential documents on their desks to prove that I had been there and left without getting caught.










Most of our assignments start with clients telling us that we will never get past their security systems. We prove them wrong at least 90% of the time. I have been able to access all sorts of places, including a bank vault and a maintenance hangar at an airport.



Barry Thomson is a senior consultant employed by Sneektheef, a security company. The company's activities are perfectly legal. Clients' boards commission the company to look for weaknesses in their systems and to attempt to exploit those weaknesses to obtain access. Clients' staff are not warned that such a check has been planned.

 Reference Material Pre-seen

Draft your response to Sabine's requests in the box below.

       **B** *I* U  x_2 x^2 

Paragraph ▾  ▾        

 Reference Material Pre-seen

A week later, Saefwell's Board is still considering offering the service of penetration testing of physical security systems.

You receive the following email:

From: Sabine Anselm, Chief Finance Officer
To: Senior Finance Manager
Subject: FWD: Sneektheef

Hello,

I am forwarding an email that I received from Bai Jing.

The Board will meet soon to discuss Bai's recommendation.

I need your help with two matters:

- Firstly, evaluate the arguments for and against the acquisition of Sneektheef as opposed to Saefwell creating its own physical penetration testing business.

[sub-task (a) = 50%]

- Secondly, identify and evaluate the challenges associated with negotiating the exchange of shares with Sneektheef's founder.

[sub-task (b) = 50%]

Regards

Sabine

The email referred to by Sabine can be viewed by clicking on the Reference Material button above.

From: Bai Jing, Director of Physical Security Services

To: Sabine Anselm, Chief Finance Officer

Subject: Sneektheef

Hello Sabine,

The Chief Executive asked me to speak to the owner of Sneektheef, the consulting firm that offers penetration testing of physical security systems. Sneektheef is unquoted and maintains a low profile, so little was known about it. They employ 150 consultants, rather more than we had expected.


Sneektheef is owned by Maria Accame, who founded the company 10 years ago after working as a freelance security consultant. The company has grown steadily under her leadership and she now plans to step down and retire.

Maria would be prepared to exchange 100% of Sneektheef's shares for shares in Saefwell, with the number of Saefwell shares to be agreed.

I intend to recommend to the Board that we acquire Sneektheef.

Regards

Bai

 Reference Material Pre-seen



Draft your response to Sabine's requests in the box below.

From: Senior Finance Manager

To: Sabine Anselm, Chief Finance Officer

Subject: FWD: RE: Sneektheef



 Reference Material Pre-seen

Six months have passed. Saefwell has acquired Sneektheef and is now offering penetration testing of physical security systems across Barrland.

You receive the following email:

From: Sabine Anselm, Chief Finance Officer
To: Senior Finance Manager
Subject: Training of penetration testing consultants

Hello,

I have attached an extract from the minutes of this morning's Board meeting.

I am interested in your opinion on two matters:

- Firstly, recommend with reasons how Saefwell could report its training programme as intellectual capital and human capital. Your recommendation should ignore the issues arising from the two incidents.

[sub-task (a) = 40%]

- Secondly, recommend with reasons the work that Saefwell's Internal Audit Department might undertake in order to ensure that Saefwell's staff are not breaking the law when they undertake penetration testing assignments.

[sub-task (b) = 60%]

Regards

Sabine

The extract referred to by Sabine can be viewed by clicking on the Reference Material button above.

Extract from Board minutes**Training of penetration testing consultants**


Bai Jing, Director of Physical Security Services, informed the Board that integration of Sneektheef into the Saefwell Group is progressing well. Sneektheef did not lose any of its consultants during the acquisition and demand for its services have grown. The company is struggling to satisfy demand for penetration tests.

Bai Jing has responded by seconding 20 of Sneektheef's consultants to provide training courses for groups of Saefwell's experienced security guards. This training will increase the Group's capacity for penetration testing assignments.

These training courses have been time consuming because of the wide variety of techniques that Sneektheef's consultants have developed in surveillance and in deception in order to obtain access to clients' premises.

The first batch of former security guards has recently started work in their new role. Unfortunately, there have been two incidents in which those newly-trained consultants have broken the law:

- A client's premises were breached by accessing a neighbouring warehouse belonging to a third party and breaking a window leading to the warehouse roof to gain access to the target building. The third party is pressing to have the consultants arrested and charged with burglary.
- A security guard employed by a different client was locked in a cupboard by a consultant. The guard was not injured but has insisted on pressing assault charges.

 Reference Material Pre-seen

Draft your response to Sabine's requests in the box below.

From: Senior Finance Manager

To: Sabine Anselm, Chief Finance Officer

Subject: RE: Training of penetration testing consultants





Thank you for completing the Strategic Case Study Exam.

Before you leave, don't forget to collect your printed confirmation of attendance.

Please click the End Exam (E) button before leaving the testing room quietly.



AICPA® & CIMA®

Together as the Association of International
Certified Professional Accountants

STRATEGIC CASE STUDY

MAY & AUGUST 2024

EXAM ANSWERS

Variant 1

These answers have been provided by CIMA® for information purposes only. The answers created are indicative of a response that could be given by a good candidate. They are not to be considered exhaustive, and other appropriate relevant responses would receive credit.

CIMA will not accept challenges to these answers on the basis of academic judgement.

SECTION 1

Requirement 1 – Stakeholders

Wavhull's shareholders will have an interest in Saefwell's decision because the investigation could have significant implications for their confidence in the integrity of their directors. Depending on the outcome of the investigation, it may be necessary for Wavhull's Chief Executive to resign or for him to be dismissed on the grounds of misconduct. Confidence in the Chief Executive could be undermined if Saefwell's consultants inadvertently reveal the purpose of their investigation. There could be a significant financial loss to Wavhull, which will affect the wealth of its shareholders, if the investigation leads to the cancellation of Company X's order. In the event that the investigation reveals that a bribe was paid, then Wavhull will have to inform the Board of Company X of the dishonest payment and that would put Company X under extreme pressure to cancel the contract. Company X's shareholders will also have to bear the cost of the assignment, which is likely to prove expensive. Saefwell will have to gather a great deal of evidence, all of which will have to be studied carefully and corroborated.

Saefwell's shareholders will be affected by this decision because of the significant risks and rewards that this assignment creates for their company. There is a possibility that Saefwell's report will conclude that Wavhull's Chief Executive was responsible for a serious act of bribery. Such a conclusion could be challenged by the Chief Executive which could lead Saefwell being accused of negligence. Saefwell could suffer reputational damage from any such challenge in the short term, although there could be a long-term benefit if the company mounts a robust response to any claims for damages. This could be a high-profile assignment that will add to Saefwell's reputation simply through association with such a large case of wrongdoing. That benefit is, however, conditional on the team's findings. If Saefwell's investigation clears Wavhull's Chief Executive of any wrongdoing, then the results will undoubtedly remain confidential. The client will not wish to be associated with bribery allegations unless they are proved. Refusing this assignment will involve an opportunity cost in terms of

lost revenue. The consultants who could have been profitably engaged on this assignment might otherwise be idle, but still in receipt of salaries.

Saefwell's consultants will be affected by the decision to accept this assignment because it will be a difficult investigation to complete under the circumstances. The limited information in the Board minutes suggests that it will be difficult to gather convincing evidence of any wrongdoing, which will put the consultants in a very difficult position. It appears that the B\$8 million payment was made to Company Y and that the payment was authorised by the Chief Executive, so there are no obvious avenues of investigation. The payment appears to have been authorised by the Board, otherwise the Non-Executive Chair would not have been aware of it. Saefwell's consultants are restricted by the need to investigate the bribery accusation under the pretence of conducting a risk assessment, which will restrict the types of question that can be asked. It will also be difficult to conduct the investigation without obtaining the cooperation of the senior management of Company Y, which is unlikely to be forthcoming given that Company Y has been accused of being implicated in the bribery.

Requirement 2 – Ethical implications

Accepting this assignment will require Saefwell to comply with the principle of confidentiality, after Wavwell's Non-Executive Chair made the award of the assignment conditional upon concealing the purpose of the investigation. Saefwell's management team will have to ensure that it will be possible to undertake a satisfactory review without disclosing its purpose. Managers and staff at Wavhull could infer a great deal from the questions that the consultants are asking. Ideally, Saefwell's consultants should ask for an opportunity to inspect the documents and papers relating to the "technical advice" allegedly purchased from Company Y and for the correspondence with Company X. It would be unethical for Saefwell to accept this assignment unless it was possible to form a clear conclusion about the likelihood that bribery had occurred without engaging with staff at Wavhull. If the need to preserve confidence will make the assignment impossible to complete, then Saefwell should warn the Non-Executive Chair that this constraint will have to be removed at some point in the investigation.

Saefwell could be accused of lacking integrity because it is being asked to mislead the subjects of its investigation about the nature and purpose of the work that is being undertaken. This investigation is looking into the possibility that Wavhull's Chief Executive has committed a criminal offence by bribing a director at Company X. The Chief Executive may not necessarily have acted alone and so there could be others who are under investigation for dishonesty. If Saefwell's consultants lie about the true purpose of the investigation, then Wavhull's staff could unwittingly reveal that they were involved in an act of bribery and so they could leave themselves exposed to criminal charges. This approach to the assignment could be viewed as denying the Chief Executive and others, including Wavhull's Cashier, of the rights afforded by criminal law, such as the right to be cautioned before being asked potentially incriminating questions. By acting in this way, Saefwell's consultants could render any evidence that is gathered inadmissible in court and so guilty parties could escape conviction. It could, however, be argued that the Non-Executive Chair has the authority

to specify the manner in which the investigation is to be conducted and the approach that is to be taken to engaging with the Chief Executive and staff.

It will be very difficult to conduct this investigation in an objective manner. The consulting team will be hoping to find evidence that incriminates the Chief Executive and may evaluate the evidence with that in mind. The Non-Executive Chair has come to Saefwell with a strong suspicion that the Chief Executive has committed bribery and with circumstantial evidence, including the fact that a large payment was authorised verbally. There are strong grounds to suspect that the Chief Executive is guilty and that a satisfactory investigation will uncover the Chief Executive's guilt. If the consultants fail to prove a case against the Chief Executive, then there may be a concern that they have failed to achieve the outcome expected by Wavhull's Non-Executive Chair. It will also be easier for both the Chair and for Saefwell itself to defend any accusation of defamation by the Chief Executive if the consultants prove a case of bribery.

SECTION 2

Requirement 1 – Internal audit review

The investigation has reached a point where the consultants will have to reveal their true objectives if they are to proceed further. That could expose Saefwell to risks of reputational damage if the Chief Executive is offended by the investigation and takes action against Saefwell. Having the Internal Audit Department review the files of the investigation to date will provide Saefwell's Board with some assurance that the investigation to date has been conducted in accordance with the company's policies. Internal auditors are experienced at checking for compliance with established procedures. In this case, that could include checks that work has been properly reviewed by senior consultants and that all findings to date have been supported with sufficient evidence. The Board could commission an internal audit review in order to be certain that there will be no unpleasant surprises if Saefwell's findings are challenged in court by Wavhull's Chief Executive. Internal Audit staff are in a stronger position to undertake this review than anyone else within Saefwell. A second team of consultants could read the files, but they would not have the same level of independence as a team of internal auditors. Auditors are also experts in the evaluation of evidence, checking that it is sufficiently persuasive to satisfy the objectives of an audit.

There is a risk that involving the Internal Audit Department will demotivate Saefwell's consulting team. Consultants in a major security team should be capable of evaluating the strength of any case that they have compiled against a suspect who has been accused of wrongdoing. It could be that requesting support from Internal Audit will create the impression that Saefwell's Board lacks trust in its consultants. It may be preferable to have the head of the consulting team talk to the Board through the strengths and weaknesses of the findings to date. The consultants are experts in conducting this type of investigation and so will be aware of the different directions that could be followed if work is to progress. Internal auditors are better equipped to study the work that has already been undertaken. There is a risk that involving Internal Audit in consultancy assignments will undermine auditor independence in relation to operational matters. Furthermore, this review will also distract Internal Audit from its programme of audit activities. Overall, this could have a negative impact on Saefwell's governance.

Requirement 2 – Share price

The share price reflects the stock market's expectations of Saefwell's future cash flows. The share price will respond to any change in the market's expectations concerning cash flows. The share price will fall if the market interprets these rumours as implying that Saefwell is in danger of exposing itself to a serious and damaging legal challenge. If Wavhull's Chief Executive responds aggressively to rumours of this investigation, then Saefwell could be forced to pay compensation, which will reduce the share price if the compensation is substantial. A claim by the Chief Executive could also distract Saefwell's management team from the tasks of obtaining and completing assignments. The impact of this rumour could be temporary because it is unlikely that any compensation will be sufficient to have a significant effect on Saefwell's financial performance. In that case, the share price may dip while the market digests that news,

after which time it will probably recover. The dip could be due to either uncertainty or because of speculative forces, with market participants selling shares in the expectation that the price will drop, which would push prices down. Those speculators would then have to buy shares to cover the positions, which would push the share price back up.

The rumour could cause more permanent damage to Saefwell's share price if it was interpreted as having the potential to cause a decrease in future revenue. If it becomes public knowledge that Saefwell misled Wavhull's staff about the real purpose of its investigation, then potential clients may be reluctant to appoint Saefwell in the future. The presence of Saefwell consultants could unsettle staff at all levels if they believe that they may be under investigation for wrongdoing, despite being assured that the investigation is focussed on company performance. Saefwell is in competition with other security companies, so there are alternatives in the event that a board is reluctant to appoint it. The impact of this concern will depend, at least in part, on Saefwell's ability to reassure corporate clients that it will be truthful about the reasons for the presence of its consultants. If Saefwell is open about the possibility of lost business and offers a convincing response to that possibility, then the market may be reassured that there will be little or no loss of business and so the share price will not decrease. The market may be prepared to accept that it is not unusual for security companies to be forced to mislead the subjects of their investigations and so the events at Wavhull could be a normal part of business for any consultancy.

It is possible that the market will regard it as positive news that Saefwell has been entrusted with a significant contract to investigate an important governance issue at a quoted company. Saefwell would not have made a public announcement of this appointment because it would have been keen to maintain a low profile, given the circumstances. Wavhull is a quoted company and an appointment to investigate its governance would be prestigious and so should enhance Saefwell's reputation as one of the leading security companies. The investigation into whether Wavhull's Chief Executive is a challenging assignment and so there is a reputational benefit associated with this appointment. Again, that could help the company to win further business. The market might, however, be concerned that the rumours that are circulating could be blamed on carelessness by Saefwell during its investigation. It is clear that the work being undertaken should be carried out under conditions of secrecy and so Saefwell should aim to reassure potential clients that it was not responsible for whatever leaks led to the rumours to emerge. Again, the impact on the share price will depend on whether the market is reassured that Saefwell will emerge with its professional reputation intact.

SECTION 3

Requirement 1 - Laubooker acquisition

Laubooker provides a specialised service that would add value to the Saefwell Group. Saefwell's consultants can carry out investigations, but they do not necessarily have the expertise to evaluate whether their files would be sufficient to obtain a criminal conviction. It may not be sufficient to take legal advice because it may be difficult for lawyers to fully understand the nature and quality of the evidence. They may not always know the correct questions to ask. The Wavhull case demonstrates that difficulty because lawyers were unable to evaluate the strength of the evidence obtained from the bribery investigation. The fact that Laubooker's professional staff are qualified in both accountancy and law enabled them to make a clear and supportive recommendation that gave Saefwell a direction for the Wavhull case. Laubooker has clearly invested heavily in recruiting professional staff who are double qualified as both accountants and lawyers. There are relatively few professionals who hold double qualifications. Presumably, Laubooker also has extensive experience of advising on the legal issues arising from forensic accounting investigations, otherwise there would be little point in maintaining its staff of professionals.

Acquiring Laubooker could enable Saefwell to claim expertise that cannot be matched by rival security companies. Potential clients may be attracted by the fact that Saefwell can call on the support of these specialists. It is unlikely that many rivals will have such access. Rivals will find it difficult to recruit suitably qualified professionals to create their own capability. Hopefully Saefwell will be able to create additional publicity for its successes by pressing more clients to pursue court action against wrongdoers, or by taking more aggressive action such as dismissing errant board members, who might otherwise be encouraged to resign quietly. If Saefwell wins a few such victories for its clients, then it will be able to press for concessions without necessarily having to take matters to court. Its enhanced reputation will be sufficient to provide its clients with an advantage.

Saefwell could avoid the cost of making an acquisition by simply continuing to use Laubooker, paying a fee for services rendered. It may be possible to pay an annual retainer, which will ensure that Saefwell receives priority treatment when an assignment requires Laubooker's services. Laubooker occupies a niche that relies on specialist consultants. Saefwell may not have sufficient work of this nature to justify ownership of the company. Keeping Laubooker's consultants occupied could prove a distraction that leads to Saefwell advising clients to pursue legal remedies instead of more logical alternatives. It may be sufficient to compromise by recruiting a small team of consultants who hold a dual qualification in law and accounting.

Saefwell's clients will often be reluctant to pursue legal action because that might draw attention to an issue that they wish to remain confidential. For example, Wavhull's Board may have been happier for its Chief Executive to resign quietly in the event that there is evidence of bribery. That might be preferable to reporting the offence to the authorities and having the matter tried in the criminal courts. There may be a small number of cases in which clients require legal advice from an organisation such as Laubooker, but those cases can be addressed by subcontracting legal work to an independent firm. Having Laubooker in house and making extensive use of its advice could create ethical problems for qualified lawyers who uncover evidence of illegal

activities. Clients may be reluctant to appoint Saefwell if they are at risk of being pressed to report matters to the authorities.

Requirement 2 – Post acquisition

The relationship between Laubooker's founders and Saefwell's Board could create significant problems if they disagree about the manner in which the company should operate as a subsidiary within the Saefwell Group. For example, the founders' desire to maintain a low profile might not be shared by Saefwell's Board, who might view the acquisition as an opportunity to raise the profile of this service. There could be other sources of conflict between Laubooker and the Saefwell Group. Saefwell is a security company, while Laubooker is a forensic accounting firm. There could be different professional obligations associated with the two activities. Laubooker's professional staff will have to comply with the obligations imposed by both their accounting and legal qualifications. Saefwell's consultants will not necessarily hold professional qualifications and so may have greater freedom in their operations.

It seems strange that the founders are keen to retain a significant, but non-controlling, interest. That could create difficulties with regard to the strategic management of Laubooker within the Saefwell Group. The founders will have a strong incentive to maintain the value of their shares, while Saefwell's Board will be more interested in the value of the Group as a whole. There could be difficulties associated with internal charges for joint assignments in which risk consultants work alongside Laubooker's staff. It will be difficult for the founders to sell their remaining equity to third parties, which could create difficulties in terms of preserving an exit strategy should the need arise.

Laubooker's value is heavily dependent upon the retention of its 120 professional staff. There is no guarantee that they will wish to remain with the company after the acquisition. At present, they work for the four founders, all of whom share their backgrounds as double qualified lawyers and accountants. They may feel less valued when they are working within a much larger, and more conventional, security company. The consultants could also be open to advances by rival security companies who are keen to create their own equivalents to Laubooker. Saefwell could be forced to increase salaries in order to prevent these professionals from being head hunted by third parties. That could create further difficulties because its risk consultants may resent an increase in salaries for Laubooker staff unless their salaries are also increased.



AICPA® & CIMA®

Together as the Association of International
Certified Professional Accountants

STRATEGIC CASE STUDY

MAY & AUGUST 2024

EXAM ANSWERS

Variant 2

These answers have been provided by CIMA® for information purposes only. The answers created are indicative of a response that could be given by a good candidate. They are not to be considered exhaustive, and other appropriate relevant responses would receive credit.

CIMA will not accept challenges to these answers on the basis of academic judgement.

SECTION 1

Requirement 1 – Share price movements

Capital markets are generally believed to be efficient, which means that share prices reflect the information that is available to the market. The stock market was aware that companies were exposed to risks associated with digital security and share prices reflected the market's estimates of those risks. The share price has fallen slightly for the companies who have volunteered the additional disclosures, which suggests that the markets have been optimistic in terms of estimating this vulnerability. The additional information in the voluntary disclosures suggests that digital security problems are worse than the market had understood, and so the share price has fallen to reflect the market's better understanding of the problem. The fact that all prices have fallen suggests that the market was unable to infer the extent of the vulnerability without the new disclosures. The voluntary disclosures have enhanced the market's understanding and so share prices have fallen.

The companies who chose not to offer a voluntary disclosure have suffered a much larger decrease in share price. That suggests that the market is reading a great deal into the decision not to publish that information. It is reasonable to anticipate that the decision to volunteer this disclosure was influenced by the extent to which companies are faced with risks relating to digital security. The stock market appears to believe that companies who have withheld this report have done so because they are faced with greater risks than the companies who have reported. The reporting decision is being interpreted as a signal, with companies who have less to be concerned about volunteering disclosure to distinguish themselves from the companies who are at greater risk. It remains to be seen whether the market's reaction to non-disclosure is excessive. It would be interesting to see whether companies could reverse some of the decrease in their share prices by offering a separate report on digital security. Companies who believe that their share prices have been depressed could arrange analyst briefings at which they disclose the facts relating to digital security events.

Overall, the share price reaction suggests that all companies should recognise that the stock market regards information about digital security breaches as significant. Share prices respond to information because breaches are believed to be capable of affecting future cash flows. Keeping the market informed is, therefore, a matter of good governance. Companies should take this into account when developing their digital security strategies. Investing time and money in effective security systems will benefit the shareholders by boosting share prices. It will also be beneficial to keep the stock market informed, provided that it is possible to do so without revealing information that could be helpful to potential intruders. Companies should also consider exceeding the minimum reporting requirements in order to signal that their systems are well designed. Doing so could be viewed as a positive signal that increases the share price.

Requirement 2 – Governance issues

Assigning ownership of the risks associated with digital security will be difficult because it is unlikely that any of the directors will be keen to accept responsibility. Success in this role may be taken for granted because shareholders will expect the Board to take care over the management of IT controls, so little credit will be given for protecting Saefwell's systems. Conversely, any successful breaches will reflect badly on the director who has been held responsible. Directors will be reluctant to hold positions in which success is not rewarded but failure is punished. One response would be to share responsibility for digital security between two directors, with each having specific responsibility to ensure that duties are not overlooked. The Director of Legal, Risk and Business Ethics should be in overall charge of managing all risks facing Saefwell, taking responsibility for managing digital security at a strategic level. The Director of Intelligence-led Security Services should provide all technical support required to manage digital security, ensuring that Saefwell makes good use of the resources that are available to it to manage this vulnerability.

Hackers who wish to breach digital security have the initiative, putting the companies defending against intrusion attempts at a disadvantage. They are constantly developing different techniques to probe for weaknesses in systems. There is a strong possibility that these constant attacks will succeed because of the discovery of a previously unidentified vulnerability. That vulnerability could be highly technical, such as a coding error in an operating system, or a simple matter such as a member of staff being tricked or bribed into disclosing a password. From a governance point of view, it should be made clear that blame will not be apportioned for breaches unless they are the result of dishonesty, incompetence or recklessness. The Board could commit itself to investigating the cause of any breach before any consideration of blame. If that investigation reveals that all reasonable precautions had been taken and that the breach could not have been foreseen, then the Board should support the director who was responsible for that aspect of security.

A successful digital security strategy could prove expensive because there will be little to show for any investment in controls. Shareholders will not necessarily view expenditure on digital security as justified. Managers might be reluctant to invest additional time and money in order to enhance security because of potential criticism for wasting resources. That could be addressed in part by classifying research and development of enhanced digital security techniques as being a key part of Saefwell's business activities. This work will be of value in assisting clients. These costs can also

be justified on the grounds that Saefwell's credibility as a risk management company will be lost if it is the victim of a major breach. The new disclosures relating to breach attempts against quoted companies will give Saefwell an opportunity to publish detailed analysis of the nature of the breach attempts that have had to be repelled. That could even encourage potential clients to spend more on Saefwell's services.

SECTION 2

Requirement 1 – Acquisition

The new disclosure rules will probably create opportunities such as additional demand for advice and support relating to digital security. Potential clients will wish to be able to offer credible disclosures concerning their ability to identify and manage both attempted and successful breaches. The need to make these disclosures will almost certainly require improvements to systems and the ability to interpret the output from security software, which may require consultancy support. Irnbyte's background is a good match to the demand that is likely to arise from these new disclosure requirements. The company has a large number of consultants who specialise in advising on digital security and so they will be well equipped to evaluate the impact of attempts to breach client systems. Having the consultancy staff available will enable Saefwell to be more responsive in relation to client requests for support. The increased awareness of digital security will mean that clients' directors will perceive the need to respond quickly to events. If a breach reveals a potential vulnerability, then they will wish to be able to report that the weakness has been addressed.

The fact that the consultants are located in Renoland should not affect their suitability for supporting clients who are concerned about their compliance with the new disclosure requirements. It is possible to access and interrogate client systems remotely from anywhere in the world. Irnbyte's consultants can easily support disclosure requirements from Renoland. There are no real disadvantages to offering this service remotely, unlike other types of digital security service such as penetration testing using social engineering, which may be difficult to undertake remotely. Saefwell could create a niche business in dealing with disclosure requirements and advising on whether systems are capable of addressing attempted breaches. If Renoland's weaker economy means that salaries are cheaper then, the Saefwell Group may be able to undercut fees charged by rivals based in Barrland in supporting clients.

There could be a threat associated with using Irnbyte to review attempted breaches on clients whose systems have previously been developed or tested by Saefwell. Clients may be dissatisfied if Irnbyte classifies an attempted breach as capable of defeating the controls that are in place at Saefwell's recommendation. If breaches are reviewed by the consultants who originally advised the client, then any advice relating to the findings can be tailored to avoid risking damage to Saefwell's reputation. For example, the report could focus on the possibility that the breach attempt used a newly-developed technique that has only just been identified by the security industry. Irnbyte's consultants might be unwilling to phrase their reports in a manner that is supportive of the advice that has already been offered by the Saefwell Group.

If Irnbyte's consultants are successful in assisting Saefwell to win additional business in this niche, then rival security companies might respond by recruiting them. It may be possible to persuade Irnbyte's consultants to move to another firm in return for a higher salary. Any attempt by Saefwell to resist such an attempt will almost certainly push up its payroll costs. Alternatively, Irnbyte's consultants might struggle to adapt to the requirements associated with advising Barrlandian companies about disclosure requirements. Renoland has high educational standards, but it may have a different culture with regard to governance and so Irnbyte's consultants may not be particularly well equipped to address clients' needs.

Requirement 2 – Currency risks

The basic concern is that Irnbyte's operating costs will be incurred in R\$, while the revenues will probably be invoiced to clients in their local currency, the B\$. If the R\$ strengthens, then the cost of consultants' salaries will increase when converted to B\$. If contracts are priced in accordance with prevailing exchange rates, then Saefwell could suffer economic risks arising from the fact that clients will have to pay more if the R\$ is strong and so they may be discouraged from employing the Saefwell Group rather than a rival security company. Once a contract has been agreed, then Saefwell could suffer transaction risks because the B\$ could weaken further against the R\$ and so there would be less cover for the salary costs that will be incurred by Irnbyte.

It would be helpful for Saefwell to evaluate the volatility in terms of historical data. Historical ranges in exchange rates could persist and so the Board would have a reasonable idea of the "best" and "worst" possible cases in terms of potential outcomes. This data might also offer an insight into the extent to which the governments of the two countries may act to avoid excessive changes in their currencies. Saefwell's Board can also obtain an insight into market expectations of future rate changes by comparing forward rates with spot rates and by comparing interest rates offered in both countries. Those forecasts will not necessarily prove accurate, but they are a credible starting point for any predictions of future movements and volatility.

It may be that the best way to deal with these currency risks would be to accept them. If Saefwell works on the basis of an "average" exchange rate when pricing contracts, then it is to be hoped that gains and losses will even themselves out in the long term. There are unlikely to be viable alternatives. Pricing contracts in R\$ would have the effect of passing currency risks onto clients, which would benefit Saefwell with respect to contracts that it wins but would risk the loss of business. The only other possibility would be to persuade consultants to relocate to Barrland, which would mean that costs and revenues would be denominated in B\$. That would, however, be a major step for Irnbyte's consultants and could lead to resignations.

The acquisition of a foreign subsidiary could increase Saefwell's exposure to translation risk. Translation gains and losses rarely affect cash flows and so they should be accepted.

SECTION 3

Requirement 1 – Reporting performance

Ideally, boards should highlight the proactive responses that their strategies include for the management of digital security risks. For example, they might disclose the fact that they hire security consultants to review and test their systems to ensure that all necessary controls are in place. Investing in such support will demonstrate a commitment to effective security. The strategy should be described in sufficient detail to enable shareholders to understand the extent to which their directors are addressing those risks, but should not be detailed enough to assist potential intruders to break into companies' systems. It may be helpful to list precautions that are taken, such as ensuring that all software updates are downloaded and installed as soon as they become available. Disclosing such controls demonstrates an awareness of the issues that can affect security.

It might reassure shareholders to disclose numbers and values that reflect a commitment to sound digital security. For example, knowing how much the company spends on updating and enhancing its software will reflect the extent to which the company values this aspect of governance. Shareholders may find it reassuring to compare such disclosures from company to company, even if the numbers do not necessarily reflect the risk or the effectiveness of its mitigation. These disclosures are unlikely to assist hackers to identify weak companies because spending money on security is not, in itself, a sign of a strong company. A breakdown of, say, staff numbers will be unlikely to assist hackers plan for successful attacks.

Companies should classify the number of attempted breaches, breaking them down into helpful categories that inform shareholders of the nature of the risks that they face. The ability to offer a clear and logical classification will demonstrate the ability to understand and appreciate the nature of the threat that is being faced. It will also make it easier to describe the extent to which the strategy can withstand breach attempts. Care should be taken to avoid informing hackers of potential weaknesses in the strategy. For example, if the attempts are classified according to the techniques being used, then hackers might identify areas where the company is weak. Statistics might reveal the areas in which the company's systems are weak because it may not detect a particular type of attack and that might encourage more targeted attacks.

Requirement 2 – Reportable attempts

Company boards should comply with the principle of professional behaviour, which implies both compliance with relevant laws and regulations and avoiding bringing the entity into disrepute. The regulations requiring disclosures should be studied carefully to ensure that any definitions of reportable events are identified and complied with. It seems unlikely that the Stock Exchange would impose strict regulations without defining key terms or setting out the disclosures that are expected. Even if the regulations define reportable events, that definition is likely to require some degree of interpretation. It is important that the rules are interpreted in a realistic manner that does not exploit any requirement for professional judgement in their application. Companies who abuse any ambiguity in reporting are likely to undermine their own credibility.

The directors should consider the need for confidentiality in reporting. Care will have to be taken to ensure that the report does not divulge any facts or other information that is subject to conditions of secrecy. For example, disclosures should not breach the terms of contracts with consultants or software providers concerning the ability of proprietary products to deal with an attempted breach. Breaching contractual agreements would be unfair to the providers of security services and could also mean that companies will be unable to obtain access to the latest and most effective security products. Excessive detail about the attempted breaches that have been discovered could equip potential intruders to improve their chances of making successful breach attempts in the future. There is clearly a potential conflict between shareholders' need for information and their need to be protected against losses through the publication of details about security.

The principle of integrity requires companies to be straightforward and honest when making these disclosures. That means that there should be clarity about what is actually disclosed. It may be that the regulations do not define reportable events with absolute clarity. It may be difficult to do so because of differences between different types of business and the nature of their systems. In that case, companies might assist shareholders by defining reportable events for themselves and publishing their definitions. Doing so would go a long way towards transparency in reporting, allowing directors to define events in a manner that makes them accountable to the shareholders. Over time, such disclosures would enable companies to develop effective standards for reporting on digital security.

Objectivity is important because directors should be discouraged from manipulating disclosures concerning data security to meet their own interests. It could be argued that disclosing any information about attempted data breaches will assist and encourage potential intruders and so directors might be reluctant to identify all events. It has, however, been determined by the Stock Exchange that shareholders are entitled to receive this information. That is sufficient to indicate that the shareholders should be kept informed regardless of the potential problems that might arise. The problem is that the number of attempted breaches could be a misleading statistic, despite its objectivity. For example, large numbers of attempts could be made against an attractive target such as an online bank but many of those attempts are likely to be ineffective because they use crude techniques that are almost certain to fail. Disclosing the raw data could be less informative than a report that classifies attempts according to the sophistication of the attack and its likelihood of succeeding.



AICPA® & CIMA®

Together as the Association of International
Certified Professional Accountants

STRATEGIC CASE STUDY

MAY & AUGUST 2024

EXAM ANSWERS

Variant 3

These answers have been provided by CIMA® for information purposes only. The answers created are indicative of a response that could be given by a good candidate. They are not to be considered exhaustive, and other appropriate relevant responses would receive credit.

CIMA will not accept challenges to these answers on the basis of academic judgement.

SECTION 1

Requirement 1 – Political risks

There is a risk that the Neerlandian Government will instruct the country's authorities to strictly enforce the rules in the case that has just been reported. Saefwell is a foreign security company that is technically in breach of Neerland's data protection laws. The Justice Minister may wish to appear assertive in protecting citizen's rights to privacy. If that is the case, then there is a strong possibility that any enforcement action will be publicised and so Saefwell's reputation may be damaged. The press could treat this as a major story, focussing on Saefwell rather than the more general question of siting security cameras and so might look for more cases where Saefwell has cameras that breach the rules. Clients may start to question whether the company has breached the regulations in protecting their premises and could press for expensive modifications to security systems installed by Saefwell.

The spokesperson's comment suggests that Saefwell has been taking advantage of weak enforcement of the regulations to position cameras to maximise their effectiveness. The publicity arising from this case could result in regulators taking a greater interest in protecting the privacy of individuals when they are in public spaces and taking firmer action with regard to enforcement. Ignoring this type of infringement could prove harmful to Neerland's Government, which will be seen as weak with regard to the protection of individuals' rights. Presumably, any such action would affect all security companies equally, but that could still have adverse consequences for Saefwell because clients' systems will be compromised. Removing exterior cameras or redirecting them so that they no longer capture images of the approach could mean that additional safeguards have to be implemented, such as having additional security guards staffing entrances. Such changes might undermine relationships with clients, who may be disturbed that their security systems relied on illegally-sited cameras in order to be effective.

A significant public reaction to concerns about illegal cameras could lead to the Government imposing additional penalties to enforce compliance. Penalties might involve fines or even bans on providing security services in the event of breach of the law. The whole question of personal privacy and data protection is a contentious one and so governments might feel the need to take drastic action in response to cases such as this. Hopefully, any new penalties will not take immediate effect and so Saefwell will have sufficient time to ensure that it is compliant before they come into effect. There could, however, be a significant cost if the legislation already allows for penalties that have not been imposed because of a slack approach to enforcement.

Requirement 2 – Strategy

The nature of the security industry means that clients' needs and the environment in which those needs are to be met are constantly changing. An emergent approach to strategy formulation implies that strategies can be updated in response to such changes. In the Neerland case, a change in social norms has occurred with respect to privacy and data protection. Previously, Saefwell had deliberately breached the law in order to ensure that clients' premises were secured effectively. The company now finds itself in difficulties because it is no longer deemed acceptable to use surveillance equipment to record the public approaches to private property. Saefwell will have to either modify or eliminate its reliance on surveillance systems to discourage and detect intruders. That may lead to changes in the levels of assurance that can be offered to clients or the adoption of alternative technologies that may be more expensive. It is important for security companies to avoid becoming involved in any controversy because clients will not wish to be associated with any behaviour that could harm their reputations. Ideally, Saefwell would have adjusted its strategy to take account of these social changes before the complaints concerning its CCTV cameras could be lodged. It would have been preferable to have foreseen the problem and taken steps to avoid it.

Arguably, the very nature of the work undertaken by a security company means that strategies must always be kept under review and updated in response to the threats that are being guarded against. Clients are exposed to loss or damage caused by internal and external threats that are constantly evolving and security companies must be ready to meet the new threats. For example, IT systems can be more easily breached when companies make heavy use of Wi-Fi to enable devices to communicate with one another. Saefwell can benefit from implementing an emergent strategy by taking a proactive approach to the threats that are emerging and by approaching clients to offer them options for addressing those threats. Adopting such an approach will reduce the risk of a system being breached as a result of reliance on outdated security measures. Clients will also be impressed by a proactive approach and they may be willing to pay more for a service that is updated and effective.

Care will have to be taken to avoid confusing Saefwell's strategy with the techniques that it will adopt in order to implement that strategy. Saefwell's mission statement sets out a clear strategy of providing clients with the security solutions and services that they require. It is debateable whether that broad strategy will ever have to change. It may be that strategic changes could come in the form of new services that Saefwell might provide in order to generate additional revenue. For example, the recent shift to having staff work from home creates a new set of vulnerabilities in terms of the security

of systems and the protection of data. It may be possible to win new business by alerting clients to the threats arising from home working and by offering effective solutions to those threats.

SECTION 2

Requirement 1 – Share price

In an efficient capital market, a quoted company's share price will reflect all information that is available to the market in an unbiased manner. In this case, it is unnecessary for Saefwell to make any kind of announcement for the market to infer that the company will suffer a significant expense because of the need to replace security cameras with some other form of security. The decrease in the share price is effectively the market's reaction to its own estimate of the impact that this event will have on Saefwell's future cash flows. That decrease can be partly attributed to the additional costs that Saefwell will incur in making its security arrangements compliant in Neerland, where it seems clear that it will be subject to enforcement actions. The market will also consider the possibility that Saefwell's Board will find it necessary to make corrections to its use of security cameras in other countries, either because of concerns about enforcement or because it wishes to maintain its reputation. Any announcement that Saefwell makes will be studied closely by the market. The share price will respond to announcements that lead to a correction of estimates of future cash flows.

The extent of the fall in share price could be due to speculation over the impact that the press coverage might have on the market's confidence. Some market participants might have sold shares "short" as soon as they saw the news, expecting the share price to fall still further and enabling them to buy shares at an even lower price to close out their positions. The initial, speculative sales would have caused a decrease in the share price. In time, the share price may recover if the market starts to realise that the decrease was an overreaction.

It is only the Board's opinion that the share price has fallen because of concerns about the need to spend money on additional security arrangements to compensate for the removal of cameras. That may not be the cause. The share price could have fallen because the market is concerned that Saefwell will lose clients who do not wish to be associated with adverse publicity arising from the controversy over Saefwell's attitude towards privacy.

Saefwell's beta is less than 1.0, which means that the company's equity is subject to a low systematic risk when it is held within the context of a diversified portfolio. According to the Capital Asset Pricing Model (CAPM), a security's beta coefficient determines its required rate of return. The higher the beta, the higher the required rate of return. A high beta suggests that a security is more sensitive to the economic and other factors that affect share prices in general and that the share price should reflect that higher risk. Saefwell's low beta suggests that investments in the company's equity will be less exposed to movements in the stock market as a whole and so it might be a suitable stock to include a low-risk portfolio. Looking forward, that investor can ignore the possibility of unsystematic risks that are specific to Saefwell because they have been eliminated through diversification.

Share prices are based on the market's expectation of future net cash flows for any given stock. The required rate of return used to discount those future cash flows is set in accordance with beta, but a low beta does not mean that the market will ignore news that is likely to affect expected future cash flows. Saefwell expected net cash inflows have decreased because of this event and so the share price can be expected to

decrease. The greater the reduction in cash flows, the greater the decrease in share price. The CAPM can be used to explain the behaviour of the returns on a security over the long term. Saefwell's shareholders have suffered a short-term loss because of adverse events that have to be reflected in the share price. Saefwell's Board cannot ignore unsystematic risks in their management of the company because they can have an impact on shareholder wealth.

Requirement 2 – Negative publicity

The Board is responsible for making decisions and overseeing operations at a strategic level. It would be unrealistic to expect the Board to review the security arrangements in place at clients' premises in sufficient detail to identify potential problems such as the field of view of security cameras. The Board should manage matters such as legal compliance by setting policies and ensuring that there is a sound control environment. It is legitimate for the Board to delegate the management of operational matters to the company's consultants. The consultants can seek guidance if any strategic matters emerge that require guidance from the Board.

Saefwell has an executive director responsible for Legal, Risk and Business Ethics. That director's responsibilities include oversight of compliance and Saefwell's enterprise risk management. The fact that such a role has been created indicates that the nature of Saefwell's business requires particular emphasis on ensuring that the law is complied with in all jurisdictions. The Board is ultimately responsible for everything that Saefwell does. Managers at all levels should be held responsible for reporting issues to their superiors. The Board should trust consultants and their supervisors to manage operational matters such as the siting and use of CCTV cameras, otherwise morale will be harmed.

It appears that the Director of Physical Security Services is aware that Saefwell is in breach of the law, which implies that the Board was aware of the fact that Saefwell's use of CCTV cameras is sometimes illegal. That suggests that the Board is responsible for the controversy that has affected the company's reputation. If the breach is trivial and is motivated by a desire to protect property, then it could be argued that Saefwell should have taken steps to have the law updated in response to the security needs of businesses. It is unacceptable for company boards to deliberately break the law in order to enhance their profits and so Bai's statement could be read as an admission that the Board could have foreseen the negative publicity.

SECTION 3

Requirement 1 – Ethical issues

The principle of professional behaviour requires compliance with the law. Bai Jing was aware that Saefwell was breaking the law and so had a duty to act sooner. The law might allow for different ways to achieve compliance, such as posting warning signs in affected public areas that they are under video surveillance so that individuals with concerns about their privacy could avoid them. In the absence of such possibilities, Saefwell has no alternative but to stop its surveillance of public places. There is clearly a conflict between the public's right to privacy and Saefwell's right to install security technology in order to conduct business, but that conflict has to be addressed by the law.

The principle of objectivity suggests that Saefwell should not allow its decisions to be compromised by conflicts of interest. The argument that removing cameras will put security guards at risk because they will be forced to take direct action against intruders is a distortion of the truth. The law sets an absolute standard for Saefwell's behaviour. The fact that Saefwell will choose to implement less desirable security measures in place of those cameras is irrelevant in this context. Saefwell should have complied with the law in the first place. If it is impossible to comply without risking the safety of security guards, then the company should consider stepping down from some of the contracts that it has.

The principle of integrity requires Saefwell to be straightforward and honest. Bai Jing's assertion that there was only one complaint is misleading in this context. Saefwell should not have been breaking the law. The fact that the company's decision to do so was not detected or was not reported by the public does not justify the fact that the law has been broken. Saefwell, or the security industry as a whole, could have addressed this issue by lobbying for a change to the law when the introduction of security cameras was first being considered. That is true, even if regulators chose to overlook this use of CCTV. The fact that the activity was not regarded as controversial would have made it easier to bring about the necessary change.

Requirement 2 – Internal audit

Internal Audit could start by reviewing Board minutes of meeting with Bai Jing to ensure that the purpose of the training programme is clearly understood and properly documented. The Internal Audit team should then compare the procedures manual with that documentation to make sure that there are procedures in place to deal with each of the Board's expectations of the training programme. Internal Audit staff may not have the expertise to evaluate the potential effectiveness of the procedures in themselves, but they can meet with the team that developed the procedures and can ask them to explain why procedures were put in place and why they are deemed sufficient. This is an effective audit technique that will enable audit staff to form an opinion about the credibility of the procedures. The Internal Audit team can also check for evidence that the procedures document was reviewed by suitably qualified and experienced staff and that the results of that review have been addressed. It would also be helpful to review any correspondence and reports submitted to the Board in the course of the development of these objectives, in order to identify any problems that arose and to ensure that there is evidence that those problems were addressed.

Internal Audit should review training materials, checking that they are consistent with the objectives. The Audit Team should read the training materials in some detail to ensure that they are clearly written and understandable, bearing in mind that some course participants may have no previous experience of the security industry. The materials should be comprehensive and so the auditors should check that each of the procedures has been covered. Ideally, there should be a procedures manual that can be referred to by security staff when problems arise and that should be consistent with the training materials. The manual and the training materials should be structured in order to best meet the needs of staff. The manual should be designed to enable readers to locate information quickly, bearing in mind the possibility that security staff could be under some stress when seeking guidance.

Internal Audit should review the implementation of the training programme for security staff. There should be a clear policy for the identification of participants and their needs, taking account of background and experience. All new staff should be required to complete the training before they are posted to a position of responsibility in a security team. It may be sufficient to require experienced security staff to complete limited training that deals with the changes that are being made in response to the withdrawal of security cameras. The Audit Team should download a list of security staff according to the payroll and should check that each person has been called up for training in accordance with Saefwell's policy. They should also check a sample of staff to ensure that they have submitted and passed any formal assessments and that registers show that they have been present for all relevant modules.

Internal Audit should also check a sample of security logs relating to the period after the new procedures have come into effect. A sample of incidents should be selected. The Audit Team should obtain the reports that were filed in relation to each of these incidents and should check that the new procedures were complied with. For example, there should be protocols for internal communications to summon support and for external communications to call the police or alert client management. Internal Audit should check for compliance and should also consider whether the outcome of the incidents suggest a need for change. It would also be helpful for members of the Audit Team to interview experienced security staff and to ask them about the new procedures. That might help to identify further ways in which the system might be improved.

STRATEGIC CASE STUDY

MAY & AUGUST 2024

EXAM ANSWERS

Variant 4

These answers have been provided by CIMA® for information purposes only. The answers created are indicative of a response that could be given by a good candidate. They are not to be considered exhaustive, and other appropriate relevant responses would receive credit.

CIMA will not accept challenges to these answers on the basis of academic judgement.

SECTION 1

Requirement 1 – Strategic matter

From a governance perspective, shareholders and other stakeholders view the oversight of internal control systems as a responsibility of the Board. Major corporate scandals that can be attributed to weak controls, such as Barings Bank and similar cases, have put directors under greater pressure to ensure that sound controls are in place. Governments and other regulators around the world have imposed duties through documents such as the Sarbanes-Oxley Act in the US and the UK Corporate Governance Code. The fact that directors are held responsible for the oversight of control systems indicates that internal control can be regarded as being a strategic matter. This is consistent with the fact that the quality of an internal control system is largely dependent upon the strength of the control environment. If the directors take an active interest in the system of internal controls, then that sets a positive tone with respect to internal control that affects staff throughout the company.

Saefwell is a security company and so it has to safeguard its reputation with respect to its ability to manage security threats. If the company's own systems are breached, then it will be difficult to convince clients that they should entrust their security to Saefwell. Saefwell's vision is to be "the security industry's most trusted service provider". The adverse publicity associated with a major security breach would be a major setback to the achievement of that vision. There is also the concern that a successful security breach could equip those responsible with the means to breach client systems. The company will maintain detailed files of the security systems installed at client premises and the information needed to review and maintain them, possibly including passwords that carry administrator privileges.

It could be argued that cyber security should be the responsibility of all staff at all levels regarding IT matters. While the Board should set the tone for cyber security for

managers, supervisors and staff, it should be possible to entrust basic responsibilities to junior staff. Staff at all levels should be aware of their responsibilities for simple matters such as keeping their passwords confidential. While the Board can demonstrate its interest in such matters by establishing procedures and penalising compliance failures, acts of carelessness are unlikely to be detected and the identities of those responsible are unlikely to be discovered. Cyber security could be seen to depend on the integrity and diligence of staff at all levels, not just those on the Board.

It could also be argued that the key responsibility for Saefwell's cyber security rests with the managers and staff who are responsible for identifying and managing the threats to the company's cyber security. The Board may be responsible for making decisions at a strategic level, such as staffing and resourcing internal security, but the directors require to be kept informed if they are to discharge that responsibility. The Board must be kept informed of emerging threats and of the strategic risks that require a response at Board level. The Board cannot be expected to be proactive in identifying needs for additional investment and for developing new responses. Staff from Internal Security and consultants from Intelligence-led Security Services should be advising the Board and making realistic requests for funding to enable that advice to be actioned.

Requirement 2 – Key performance indicators

Internal Security should provide the Board with a log of all cases where an unauthorised party was successful in breaching Saefwell's systems. Each event should be supported with an estimate of the extent of the intrusion, including the files that have been accessed. The log should also indicate the time taken to upgrade the system's controls to prevent that route from being exploited further. While it is unacceptable for systems to be breached, tracking the number of failures indicates the ability of Internal Security to detect intrusion. It also reports on the speed of Saefwell's response.

It would be useful to report the number of updates to operating systems and other software employed by the company to the Board. Software updates are frequently designed to remedy security concerns that have been detected by the creator of the software. A comprehensive report on the status of updates will be evidence of a proactive approach that is intended to protect systems. The report could be extended to identify packages that have not been updated recently, with an indication of the reasons for not having done so.

Internal Security could report details of staff training and updating in relation to cyber security risks to the Board. The report could include the number of staff who participated in formal training, either face-to-face or online and the nature of the topics covered. It is important that staff at all levels who use IT for any aspect of their work are trained to be aware of the latest threats and can, for example, identify the latest phishing attacks. The Board should be kept informed of the nature of the quality and the quantity of training provided both to newly-appointed staff and to staff who are continuing with the company.

SECTION 2

Requirement 1 – Stakeholder needs

Clients will have a high interest and a high power with regard to this incident. The high interest will be due to concerns that their security systems may have been rendered ineffective due to the breach. The high power is attributable to the fact that clients may demand compensation for any costs that they incur. They may also dismiss Saefwell. Saefwell will have to minimise the uncertainty by contacting clients individually, informing them of the extent to which their files may have been compromised. Clients who are now at risk should be offered advice as to how the weakness should be rectified. The cost of any such advice should be borne by Saefwell.

The Police Service will have a high interest and low power in relation to this incident. The high interest exists because the police are responsible for the investigation of the crime that has been committed against Saefwell. The Police will also have a duty to assist and protect clients who are at risk of becoming the victims of crime. The Police will have relatively little power because Saefwell has not committed a crime, and so the Police will have relatively little influence over the company. Saefwell will have to obtain permission from clients to grant the Police access to their files so that the investigation can proceed.

Members of the public will have a potentially high interest and low power. The high interest will arise because it is possible that some of the clients who have been compromised hold personal details of customers in systems that are secured by Saefwell. Customers could be at risk of, for example, having their credit card details accessed and used to make unauthorised charges or hospital patients could have their personal medical details accessed. The public will have very little influence because they will be unable to force the entities with whom they do business to change their security company. It should be sufficient for Saefwell to issue a press release that apologises to all who have been affected and advises anyone whose details may have been accessed to take particular care when doing business online.

Requirement 2 – Share price

Saefwell should start by conducting a swift internal investigation in order to identify the extent of the breach and the number of clients whose details may have been accessed. It is important that the Board can then make an informed announcement about the event, providing facts that will clarify the extent of the problem. The Board should then organise a press conference at which the media can be informed about what has happened. Saefwell should accept responsibility for the breach and should explain what it intends to do to assist clients and others who have been affected. The Board should admit that they do not yet have all of the facts and should avoid guessing or distorting the information that is available. The market will pay close attention to press coverage, particularly in the early stages. If Saefwell's Board can communicate the impression that it is in control, then the inevitable decrease in the share price may be mitigated.

Saefwell should appoint a public relations company to take over responsibility for keeping the media informed about ongoing developments with the investigation. After the initial flurry of interest, the press may become biased and may publish only negative stories, such as the discovery that personal information has been abused. The stock price may be depressed further by the publication of rumours that create uncertainty and imply that Saefwell is in difficulty. This is clearly a period in which speculators will grasp negative press coverage to profit from short selling and so anything that can be done to ensure a more balanced press coverage can only help. Hopefully, any positive news that Saefwell can release will offset that tendency.

Saefwell should negotiate with clients to encourage them to express support. The share price may be depressed because of concerns that the company will lose business. Where appropriate, Saefwell should encourage its clients to issue press releases that reassure customers and business contacts. Saefwell should assist its clients by developing tailored guidance that they may issue to their customers. If clients are making positive announcements, then they will be less likely to dismiss Saefwell. Saefwell should invest time and resources in ensuring that clients have no reason to complain about the support that is being provided. The share price will recover quickly once the market can be reassured that clients will remain loyal to the company.

Once matters have been resolved, Saefwell should invite investment analysts to a presentation at which they can be briefed about the breach. The presentation can be used to demonstrate that Saefwell is aware of the reasons why the breach occurred and so is in a position to prevent a recurrence. The analysts can also be briefed on the reliability of the system that is in place and the extent of any remaining vulnerability. The Board can also brief the analysts about the relationship with clients, including those affected by the breach. It would be appropriate to be honest about any expected loss of business. By being honest, the Board can demonstrate integrity and can hopefully discourage analysts from being swayed by any lingering uncertainties over Saefwell's future.

SECTION 3

Requirement 1 – Acquisition

Saefwell should have attempted to persuade Ramesh Kumar to remain with the company for a reasonable initial period to allow for a smooth transition. One reason for doing so would be to reassure the staff in any negotiations relating to staffing and conditions of employment. Having continuity of leadership would give consultants a trusted point of contact with regard to seeking assurances for their future. Retaining Mowrtron's Chief Executive for a period would also provide continuity of management. That would reassure clients who are waiting for software to be adapted. The loss of Ramesh Kumar could lead to clients refusing to accept completed software until it has been subject to intensive testing, which could delay the completion of these contracts. Paying a retainer to retain the former Chief Executive would also make it more difficult for him to commence work on the creation of a new business that might grow to compete with Saefwell at some level.

Saefwell should have been honest about its plans for the consultants and their job security. It is common for acquisitions to be followed by reorganisations and redundancies and so it was natural for the consultants to apply for new jobs. Saefwell's Board should have organised a briefing session, preferably in person, in which they outlined their plans for Mowrtron. They should have admitted that there will be significant downsizing after the outstanding client contracts have been fulfilled and the criteria for the selection of the 50 staff who will continue should have been announced. Ideally, a timetable should have been announced for the process of selecting the 50 consultants who will be offered continuing jobs. That would at least set a timescale for employees and would give them an insight into whether it would be worth remaining with the company in the short term. As an incentive, Saefwell should have offered a bonus to all staff who remain with Mowrtron for this initial 6-month period. That bonus should be sufficient to compensate them from applying for jobs elsewhere.

It is discouraging that the business press has paid little attention to the acquisition. Saefwell has recently been the victim of an embarrassing data security breach and it has now acquired a subsidiary that will help it to protect itself in the future. From a governance point of view, it would be beneficial for the shareholders to read about this acquisition and to see it as an investment by Saefwell in enhanced controls. It would have been possible for Saefwell to have used a public relations consultant to promote this story to business news editors and to have encouraged them to present it as a response to the recent breach. Reading such news articles would reassure shareholders that the investment in Mowrtron was being perceived as a sensible investment of their funds. Saefwell's Board should be constantly working to portray the Group in a positive manner. Apart from encouraging shareholders, it will be easier to win new business if the company can be seen to be moving forward.

Requirement 2 – Ethical implications

It could be argued that Saefwell's Board has a duty of confidence to the company and that it should not disclose any information relating to the loss of these consultants. The market is aware that Mowrtron has been acquired as a subsidiary, but there is no reason to believe that it is aware that there have been large-scale resignations. Volunteering this information could undermine the credibility of the company and could

have an adverse impact on the shareholders' wealth. There is no specific duty to disclose the news about the loss of staff. For example, there are no legal or professional duties to make this information known. It could be argued that Saefwell invested in Mowrtron in order to acquire the company's software and it has achieved that. In the short term, the loss of consultants is an inconvenience, but Saefwell can assign its own consultants to take their places or it can recruit new staff.

The principle of integrity requires the Board to be straightforward and honest in their professional relationships. Care will have to be taken with respect to its behaviour in relation to the loss of the consultants. Mowrtron has signed contracts with a number of clients who will take it for granted that the software that they have paid for will be adapted by competent experts. Saefwell's Board will have to ensure that it is capable of fulfilling these contracts in a satisfactory manner, otherwise it will compromise these clients' security. It may be possible to persuade the remaining 30 consultants to remain with the company, and their knowledge and experience of the software should be sufficient to complete the work required by the contracts. Saefwell has a duty to ensure that consultants used on any work have the necessary skills and that clients are not misled in any way. If the remaining consultants are not capable of completing the work in accordance with the terms of the agreement, then Saefwell should meet with clients and inform them of the situation. If necessary, Saefwell should cancel the contracts and refund any payments that have been made to Mowrtron.

The principle of objectivity requires the Board to conduct itself without bias. For example, the Board should not act in accordance with its own self interest. If the Board is asked a direct question about the retention of consultants, then it should either answer truthfully or it should refuse to answer at all. Shareholders and analysts may seek a response from the Board because subsidiaries often lose key staff after their acquisition and so such questions may be asked. Decisions about disclosures and responses should be based on what is best for the shareholders. The Board should aim to reassure both the capital market and the market for security services, but it should restrict itself to truthful answers. If questions are being asked in public, then it may be preferable to offer a detailed response that admits that the value of the Mowrtron subsidiary has been seriously compromised and that the Board accepts full responsibility.



AICPA® & CIMA®

Together as the Association of International
Certified Professional Accountants

STRATEGIC CASE STUDY

MAY & AUGUST 2024

EXAM ANSWERS

Variant 5

These answers have been provided by CIMA® for information purposes only. The answers created are indicative of a response that could be given by a good candidate. They are not to be considered exhaustive, and other appropriate relevant responses would receive credit.

CIMA will not accept challenges to these answers on the basis of academic judgement.

SECTION 1

Requirement 1 – Scenario planning

It would be difficult to evaluate whether the Police Service could match salaries for cyber security experts. Doing so might affect the morale of police officers from different specialisms who will be paid less than the colleagues in cybercrime. It is, therefore, debateable whether this is a credible threat to Saefwell.

At present, Saefwell can afford to exceed the salaries paid by the Police Service by a sufficient margin to encourage them to resign in order to work in the private sector. It may still be possible for Saefwell to match the enhanced salaries that are implied by the scenario under consideration. In the worst possible case, Saefwell's payroll costs will increase slightly. This could, however, become a political issue for the Barrlandian Government, who might be prepared to fund the Police Service to retain cybercrime specialists rather than risk leaving voters to bear the risk of being victims of theft and fraud.

There could come a point at which increasing salaries could reach a tipping point where newly-appointed staff from the Police Service will be paid more than Saefwell's other consultants. If Saefwell has to pay all staff more in order to compete with this one source of new consultants, then it may no longer be sustainable to do so. Saefwell may find it more cost-effective to rely on other sources.

It would be possible for the military to offer staff the opportunity to spend a year at college or university in order to graduate with a master's degree. This would augment the training that they are already receiving and would enhance their skills. Depending on how this opportunity was planned and scheduled, it might be difficult for Saefwell to recruit staff from the military even in the short term. They may extend their contracts in return for a commitment that they will be released to study in the future and so there could be a shortage of available staff for Saefwell to recruit.

Military staff might be attracted by the opportunity to study for a master's degree, which would remain on their CVs after they leave the military and so might benefit them in the long term. It might also improve their chances of promotion while still in the military. It would also be an opportunity for a different experience during their period of military service.

In principle, Saefwell could offer staff the opportunity to study for degrees, but it might still be unable to compete with the military. As a private sector organisation, Saefwell would almost certainly find it impossible to enforce a 10-year commitment to remain with the company, even in return for funding a master's degree.

It would be difficult for the government to enforce such a law because it would effectively render cyber warfare specialists unemployable in the security industry when they return to civilian life. It could lead to unintended consequences, such as discouraging people from enlisting in the military because of restricted career choices at the end of their enlistments. This would, however, be a significant setback for the security industry in terms of recruiting staff, at least for as long as such a ban remains in place.

Saefwell should develop contingency plans for dealing with an outright ban. One possibility would, paradoxically, be to recruit as many consultants as possible from the Police Service and military before the ban comes into effect. There may be other sources of applicants such as seeking staff from foreign police and military organisations. Saefwell may also be able to develop its own training programmes for recent graduates. Existing consultants could support and mentor trainees. Saefwell should also be careful to monitor the actions of rival security companies, which will face the same restrictions on the appointment of new staff from outside the industry. It will be important to ensure that Saefwell can retain its existing employees.

Requirement 2 – Political risks

Countries that are affected by the loss of cyber security professionals from their police and military are likely to be developed countries that have problems with cyber warfare and cyber crime. Otherwise, they would not have complements of cyber warfare and cyber crime experts. That could have a bearing on political risk because those countries may offer substantial markets for security companies. Saefwell might wish to do business in those countries and so it should consider taking care not to recruit too many consultants from their police and military. As a potential foreign entrant to such markets, Saefwell has to take care because there are fewer political constraints on host governments when imposing penalties on foreign companies.

One potentially significant risk is that host governments might decide not to award government contracts to security companies that have overdone the recruitment of professionals from the police and military. Government agencies are often faced with significant cyber security challenges and will have large contracts to award to security companies. Government contracts are often profitable because officials are prepared to pay more for a good quality of service. It could prove difficult for them to justify granting contracts to Saefwell or any other foreign companies that have recruited from their police and militaries.

Host governments can impose sanctions in a variety of different ways. For example, their tax authorities can investigate whether multinational companies are paying sufficient tax on the profits earned in those countries. The press often takes a keen interest in the amount of tax paid by multinational companies. There could be political pressure to investigate companies that have been the subject of some controversy, including the recruitment of staff who were trained at government expense. Tax investigations can be time consuming and can result in expensive accountancy fees, so it may be sensible not to appear to be a bad citizen.

SECTION 2

Requirement 1 – Stakeholders

Barrland's citizens will have both high interest and high power in this proposal if it is implemented. The high interest will arise from the fact that most of them will be at risk of cyber crime and even cyber warfare and so they will be affected by the quality of the service provided by Saefwell. Citizens may not take an active interest on a continuing basis, but they will criticise the Government if a security breach occurs that appears to indicate a failure on Saefwell's part. Citizens have power as voters. They may put the Government under pressure to replace Saefwell in the event of poor performance. Saefwell should ensure that all work undertaken on this contract is fully supervised and reviewed, so that the risk of compromise is as low as possible. All work done should meet or exceed the standards that would have been applied by the Police Service when it was responsible for its own security. Saefwell should be prepared to incur additional costs rather than risking the reputational loss associated with accepting risks with this key client.

The staff currently employed in a cyber security role within the Police Service will have high interest and possibly high power. The high interest will arise because transferring the responsibility for cyber security to Saefwell may mean that they will be made redundant by the Police Service. If they are serving police officers, then they may be transferred to an alternative role within the Police Service. Otherwise, they may be employed by Saefwell under different terms. Their power will depend largely on their continuing role with the Police Service. If they are not to continue with the Police Service, then they may choose not to fully brief their replacements with regard to the specific threats associated with securing police networks. Saefwell should attempt to negotiate a transitional period during which its staff can work alongside the outgoing staff. Saefwell's staff should be instructed to learn as much as they can during that period. The staff should also review all documentation relating to the system and should ensure that it is up-to-date with respect to the latest versions of software and so on. Regardless of the future employment of the existing workforce, Saefwell's team should seek one to one briefing sessions with their counterparts. These should focus on the nature of the vulnerabilities faced by the Police Service and the most effective ways of addressing them.

Requirement 2 – Suspending dividend

Suspending a dividend is potentially an effective strategy for raising equity to fund an investment. Doing so will, therefore, reduce the company's gearing ratio by increasing equity while leaving liabilities unchanged. In the process, it will also increase weighted average cost of capital (WACC) because equity is generally more expensive than debt. The alternative approaches to raising equity usually involve significant costs in terms of professional fees to ensure compliance with legal and stock exchange requirements and for underwriting. Those can be avoided by suspending a dividend. In theory, all that is required is a decision to reduce or suspend the dividend altogether and to inform the shareholders of that decision. Companies usually raise cash from their operations throughout the year in order to pay that dividend and so the timing of the funding really depends on operating cash flows.

In theory, news of this decision should lead to an overall increase in Saefwell's market capitalisation. This is partly attributable to the fact that Saefwell is retaining equity that would otherwise have been distributed and so it is avoiding an outflow of funds. There should be a further increase due to the net present value of the investment that is being made in the new contract with the Police Service. There could be some initial volatility because shareholders who rely on dividend income for personal expenditure may be forced to sell their shares. Hopefully, any such sales will not be sufficient to depress the share price and will be interpreted as being motivated by convenience.

Saefwell's Board should be free to announce that the dividend has been suspended in order to finance the investment required to undertake the Police Service contract. The stock market should interpret that as a positive sign that should result in an increase in the share price. A government contract offers security. There is little or no risk of Barrland's Government failing to meet its obligations under the contract. This is a potentially long-term opportunity for Saefwell. The Police Service's networks will always require security. It will also be desirable to have continuity in the cover that is being provided. It is unlikely that Saefwell will lose this business and so the share price should reflect the net present value of the cash flows that the contract will generate.

Some shareholders may misunderstand the implications of the behaviour with respect to the dividend and so they may sell their shares, thereby pushing down the share price. Any such decrease may be further pushed by speculators who are anticipating such an illogical reaction. If they can sell shares immediately, before nervous investors have a chance to react, they can sell at close to the current market price. The combined effects of these sales will decrease the share price in the short term, but the speculators will soon have to close their positions. The share price will start to recover once the speculators start to buy shares back. Hopefully, it will reach an equilibrium level that reflects the value of the new contract. The extent of that recovery will depend largely on the extent to which the stock market trusts the Board to deliver the benefits expected from the contract.

SECTION 3

Requirement 1 – Checking backgrounds

Candidates should be required to provide scanned copies of their certificates when they submit job applications to Saefwell. These should be reviewed for any obvious signs of forgery or alteration, such as spelling errors or inconsistencies in dates. Copies of certificates are sufficient to enable Saefwell to conduct an initial review of candidates but they are insufficient in themselves because of the risk of fabrication. Candidates who are offered technical roles should be required to provide Saefwell with the necessary authorisation to seek direct confirmation from colleges, universities and professional bodies to confirm claims of qualifications and memberships held. Direct confirmation will confirm the authenticity of these claims. Interview panels should include at least one senior subject matter expert who is experienced in the role that is being applied for. That expert should ask a number of technical questions. If candidates manage to answer the questions, then that is further confirmation that they hold the qualifications that they claim in their applications.

Candidates should be required to submit the names of at least two referees who have worked with them in a professional capacity. Candidates should designate at least one referee from their most recent employment. Saefwell's Human Resources (HR) Department should make direct contact with both referees, preferably in writing at the referee's place of employment. Reference requests should ask specific questions that require referees to demonstrate that they actually knew the job candidates. Saefwell should not accept "generic" letters of recommendation submitted by candidates, even if they appear to be on headed notepaper, because they would be too easy to fabricate. Interviews should ask candidates to explain how they would address a number of hypothetical scenarios that are aligned with the roles that they claim to have held. They should also be asked to summarise practical problems that they have addressed and resolved. The subject specialists on the interview panels will be able to evaluate the authenticity of the responses to practical questions. They should be encouraged to press for details as appropriate.

Candidates should be warned that their appointments will be conditional on them having satisfactory criminal records. They should be required to furnish details of all convictions and also of any criminal charges that have been filed against them. Making this a condition of employment will give Saefwell grounds for dismissal if it is later discovered that employees appointed under these terms have convictions and that they lied in their applications. Some countries permit employers to conduct criminal record checks on potential employees in order to identify those whose past might affect their suitability. It would also be legitimate to furnish the Police Service with names and other details of potential appointees who will be employed on the police contract and to have their backgrounds checked and confirmed.

Requirement 2 – Internal Audit

Internal Audit is likely to be objective when reviewing backgrounds. The HR Department may be under pressure to accept applicants in order to avoid criticism for delaying appointments. Once an applicant has been interviewed and found acceptable, the management team responsible for the Police Service contract may become impatient to have the reviews completed and for successful interviewees to

start work immediately. Internal Audit is not involved in operational matters and so audit staff will be able to take a more objective view, with less pressure to complete appointments to a schedule.

The Police Service has expressed concern that Saefwell's background checks have been inadequate. They may be reassured by the involvement of Internal Audit. Auditors are experts in the collection and evaluation of evidence, so their reviews of qualifications may be more credible. This change will also demonstrate to the Police Service that its complaints have been taken seriously and that Saefwell is responsive to its concerns.

Delegating the background checks to Internal Audit will enable Human Resources to focus on the process of recruiting and interviewing applicants for this role. Details of successful interviewees can be passed on to Internal Audit for checking and that will free Human Resources staff to work on the next batch of applicants. That might prove important because Saefwell has already lost time because of the 14 applicants who have been rejected by the Police Service.

There are always concerns when Internal Audit is given responsibility for an operational matter. There is a risk that its independence will be compromised because of any such activity. Internal Audit will have less credibility when reviewing any aspect of human resourcing associated with this contract. Even if audit staff are not reviewing their own work, they will be conscious of the fact that their colleagues undertook those checks. It may also be difficult to maintain independence when dealing with employees whose applications were reviewed as part of this assignment. Audit staff may be reluctant to file reports that reflect badly on the competence of the staff whose qualifications and experience they vetted.

Internal Audit has its own schedule of checks and reviews and so working on the Police Service contract will be a distraction from that schedule. This sends a dangerous message to the rest of the company because it may appear that Internal Audit is a resource that can be called on to assist other departments when they are busy or faced with difficult tasks. Hopefully, Saefwell's Audit Committee will assert itself and refuse to release Internal Audit to assist in this way. If they do not, then there could be wider concerns about the authority of Saefwell's non-executive directors.



AICPA® & CIMA®

Together as the Association of International
Certified Professional Accountants

STRATEGIC CASE STUDY

MAY & AUGUST 2024

EXAM ANSWERS

Variant 6

These answers have been provided by CIMA® for information purposes only. The answers created are indicative of a response that could be given by a good candidate. They are not to be considered exhaustive, and other appropriate relevant responses would receive credit.

CIMA will not accept challenges to these answers on the basis of academic judgement.

SECTION 1

Requirement 1 – SAF

It could be argued that this is a suitable venture for Saefwell because it is essentially a variation on the service that the company already offers. Indeed, Saefwell already conducts penetration tests on clients' IT systems as a test of their effectiveness. Saefwell currently evaluates physical security risks by studying areas of vulnerability and offering advice on controls that should address those vulnerabilities. The service provided by Sneektheef takes that a step further by evaluating the effectiveness of security systems, taking account of the vigilance and the quality of the staff who are employed to implement those controls. Saefwell's clients might be prepared to pay for such a service, partly because it will offer greater reassurance that the systems are effective if the consultants fail to breach security. Clients may also feel that it motivates employees if they know that they will face deliberate attempts to bypass security measures. They know that they will be identified in the consultant's report if they are careless. This service could create synergies that will generate additional revenues for Saefwell. The identification of weaknesses could lead to additional contracts to rectify matters. At the very least, clients might be prepared to pay Saefwell to provide staff training to ensure that loopholes in security cannot be exploited.

Shareholders might not regard this as an acceptable service because it could be viewed as unethical in many respects. In order to succeed, consultants must use deception and dishonesty in order to mislead client staff. Saefwell's vision is to be the security industry's most trusted service provider. It could be argued that a service based on deceit could undermine the company's claims to integrity. It might also be argued that the venture is based on a misleading concept of security. If a potential intruder is sufficiently motivated and has the necessary resources, then it will almost always be possible to breach a system. In the news article, for example, the security consultant had to spend a week on surveillance of the target's reception before making a move. If the reception staff had been keen and alert, then he would have had to

spend additional time on surveillance of other potential weak spots. Shareholders might also be concerned about the risks associated with offering this service to existing clients. It could reveal weaknesses that imply that the systems previously designed by Saefwell are ineffective because slight inattention could be exploited by intruders. Clients' directors may also be reluctant to commission investigations that could ultimately imply poor governance in terms of the internal controls that are in place. Also, the fact that 90% of clients believe that their systems are secure could indicate that this is very much a niche service that does not have the potential to attract a great deal of business.

The feasibility of this venture depends largely on whether Saefwell can identify and recruit suitable consultants to carry it out. All security consultants must be able to think like an intruder in order to identify vulnerabilities and to design controls that will address those vulnerabilities in an effective manner, but the service offered by Sneektheef requires consultants who can act like criminals. The consultant in the news article had the skills required to carry out covert surveillance of a reception area before striking. It was then necessary to lie in a convincing manner to be granted access to the executive floor. It could be difficult to find consultants who have the necessary skills and also have sufficient integrity to be trusted to breach client security without taking advantage for personal gain. For example, the consultant could have accessed more than three directors' offices and could have copied intellectual property or sale to a third party without Sneektheef's knowledge. The type of work undertaken by Sneektheef also requires a great deal of flexibility from consulting staff. It could, for example, be necessary to work at night or over weekends in order to identify periods when clients are most vulnerable. The consultants whom Saefwell currently employs are effectively in regular, office-based jobs and so they might be unwilling to accept assignments that require working such hours.

Requirement 2 – Risks

Consultants could be exposed to a physical risk if clients' security staff or other employees discover their presence during a breach and take physical measures to apprehend them. It is unlikely that consultants would be able to identify themselves and explain their presence in a satisfactory manner and they could be at risk from an overreaction from nervous employees. It would be difficult to mitigate this risk because clients cannot forewarn staff that a penetration test has been planned. That would undermine the value of the test because staff would be more vigilant than usual. There is also a risk that genuine intruders will be challenged and permitted to leave the premises without being apprehended because they are mistaken for the security consultants. The only effective way to mitigate this risk would be to train staff to relax and to cooperate in the event that they are challenged during a breach. Staff should also be monitored at all times when they are breaching a client's premises. There should be a supervisor who is aware of their location at all times and who has the details required to contact client staff to vouch for the consultant's credentials.

Consultants could find themselves at risk of criminal charges, even though clients' boards have granted permission for their activities. Consultants carrying out surveillance could appear suspicious to members of the public or to client staff. That could result in the consultants being arrested. The police will also become involved if a consultant breaches a property and accidentally activates an alarm. Frequent

occurrences could lead to consultants being charged with wasting police time, even though their underlying activities are intended to preserve security. If consultants are restrained in the course of their work, then they could be accused of assault if they take any action to protect themselves, even if provoked by security staff using excessive force. Client staff could also be at risk of injury from slips or falls because they are rushing to assist colleagues or simply to protect their employers. Consultants could be exposed to civil claims for compensation in the event that anyone is injured during the course of a breach.

SECTION 2

Requirement 1 – Acquisition

Acquiring Sneektheef as a going concern will potentially reduce the number of competitors in this market. It would be possible for Saefwell to start up its own penetration testing business, but it would then have to compete with Sneektheef for business. If Sneektheef's founder is keen to sell, then it would be possible for one of Saefwell's direct competitors to buy the company and expand it, making it an even more substantial competitor for Saefwell.

Acquiring Sneektheef would give Saefwell access to an existing knowledge base relating to systems and procedures that might be difficult and time consuming to create independently. For example, Sneektheef's consultants will know what steps are permissible when entering a client's premises. It may be acceptable to pick a lock, but not to use force to break a door open. Having such systems in place will save time and will also avoid the need to spend heavily on legal advice on reviewing systems and procedures manuals.

Acquiring Sneektheef will also avoid the need to recruit and train consultants to carry out this role. Sneektheef has a large staff and it may be necessary to have such numbers in order to be able to conduct surveillance without having the same individual attracting attention by being in place for too long. It may also be difficult to identify applicants with the required social skills to carry out these assignments.

It could prove expensive to acquire Sneektheef as a going concern if Saefwell cannot guarantee that it will have access to the intellectual property that is required to maintain a healthy business. The company may not have maintained detailed records of techniques and procedures and so Saefwell will have to create those for itself, which will take time even if Sneektheef's consultants are available to be interviewed on their approach. Saefwell also cannot guarantee the retention of the 150 consultants, many of whom may be unwilling to be employed by a large, quoted company that may impose more restrictions on their activities. The consultants will be potentially employable by rival companies, who may offer higher salaries in order to attract them.

There could be a significant drawback to acquiring Sneektheef as a going concern because doing so will have the effect of bringing 150 consultants into the company with no opportunity for Saefwell to check their backgrounds. There is a risk that Sneektheef's founder and senior management team took an aggressive approach to hiring and training consultants to conduct penetration tests. They could undertake assignments in a manner that is inconsistent with Saefwell's preferred approach. If Saefwell creates a company from scratch, then it will be able to take as many precautions as it wishes in recruiting staff, taking up references and conducting criminal record checks. Saefwell would also be able to set the limits on the techniques that consultants are permitted to use when conducting penetration tests.

Requirement 2 – Share exchange

Sneektheef is unquoted which means that there is no objective valuation for the company. Quoted companies have observable market prices that are a fair indication of their values. The market capitalisation would be the lowest that the seller would accept, although there could be an argument that a controlling interest is worth more

than that because the buyer can exploit any synergies. As things stand, Sneektheef's founder will be keen to negotiate the highest possible price, while Saefwell's Board will wish to minimise the cost of the acquisition. The only real limit is that both sides will have to remain credible at all times because neither will be prepared to entertain ridiculous prices and both will wish to complete this transaction. The fact that Saefwell is quoted means that its share price is known. If agreement is reached on the value of Sneektheef, then the number of shares to be exchanged can be determined by dividing Sneektheef's value by Saefwell's share price. The only further complication is that the completion of the acquisition could lead to a further increase in Saefwell's share price because of the synergies associated with the acquisition and that could have an impact on the founder's negotiating position. She could argue that she should receive additional shares because of this.

Ideally, both sides should attempt to justify a valuation that is based on a calculation rooted in finance theory. Unquoted companies are often valued in terms of models based on comparatives relating to quoted companies. The stock market values companies at the net present value of future cash flows. Future cash flows can be estimated on the basis of historical information. The required rate of return can be determined using the Capital Asset Pricing Model (CAPM), inserting the beta coefficient of a comparable quoted company in the same line of business. The difficulty here is that Sneektheef is a unique business that may not share the same systematic risk as any other. For example, Saefwell's beta coefficient could be used to attach a value to a traditional security company, but Sneektheef is in its own unique branch of the security industry and so Saefwell's beta might not be suitable.

Saefwell should also consider whether there could any post-acquisition problems that might affect the value of any investment that it makes in Sneektheef. The most obvious concern is that the company could lose much of its workforce if the consultants are reluctant to be employed by the Saefwell Group. Rival security companies who wish to compete with Saefwell could recruit consultants by offering higher salaries than Saefwell. It may prove expensive for Saefwell to retain the staff who are, after all, the only real reason for acquiring the company. It may be difficult to persuade the founder to allow for any such costs when negotiating a selling price because they reflect on the value of the company to the buyer, but not the seller.

SECTION 3

Requirement 1 – Training programme

Intellectual capital consists of knowledge-based intangibles. Saefwell will have control over organisational capital in the form of the knowledge held by consultants, both trainees and trainers, and the systems that they have developed. This organisational capital has significant value because it enables security guards to be trained as security consultants. While the security guards are intelligent people who can operate on their own initiative, they are not particularly difficult to recruit. Saefwell is capable of using its intellectual capital to scale up its penetration testing business at a relatively low cost. That intellectual capital can be controlled because the training materials are copyright, with the copyright belonging to the company. It would be difficult for rivals to replicate that material because of the wide range of skills possessed by the security consultants.

Human capital consists of competencies, capabilities and experience. Saefwell already controls those attributes as they belong to security consultants because they are subject to employment contracts. The courses that they have developed enable Saefwell to leverage those attributes in order to train additional consultants. This is significant because there are very few potential consultants with the necessary skills to conduct penetration tests available for recruitment in the labour market. Saefwell could also refer to the capabilities of its security guards in this context because they come from diverse backgrounds, including the police and military. Their previous experience means that they are capable of applying the content of the training courses to carrying out penetration test assignments in the real world. Saefwell's ability to do business is largely dependent on the skills of its consultants and their ability to learn from one another.

Requirement 2 – Internal Audit

Internal Audit could start by checking the processes followed when the training programme was developed and reviewed. The programme content should have been reviewed by a criminal lawyer to ensure that all instructions being communicated to staff are legal. The lawyer should also identify potential legal pitfalls and ensure that those are covered in the training programme. For example, the decision to restrain a security guard by locking a door could constitute assault or wrongful imprisonment. Consultants should be made aware of such matters. Consultants need to be aware of the extent to which clients can authorise their actions. A client's board can grant the right to enter property, but not to restrain employees even if no injury is caused. There should be a system in place to ensure that the training material remains up-to-date in response to changes in the law and major legal cases.

Internal Audit can review payroll records to obtain a comprehensive list of all consultants engaged in penetration testing. That list can be checked to ensure that every consultant has completed the training programme. The auditor can also review files of any assessments to ensure that only staff who have satisfactorily completed their assessments are being used in the penetration testing role. The auditor might further check on the effectiveness of the training by talking to consultants and engaging them in conversation about the legal aspects of their work. It should be

apparent from such conversations whether consultants are confident in their grasp of the legal implications of their activities.

Consultants should be required to seek approval for their plans before they carry out a breach. Supervisors should have legal training and should consider whether planned actions are legal before giving permission to proceed. Requests for approval should make specific references to the question of whether any breach will require unauthorised entry to a third-party's property or whether there is a risk of injury to client staff. Staff should not proceed without an explicit confirmation from a supervisor. Internal Audit can review the files of approval requests and responses to check that consultants are complying with this control. Audit staff could also review the responses to ensure that supervisors are responding quickly and before any action is taken.

Consultants should submit detailed records of all penetration attempts, both successful and unsuccessful, to ensure that their activities can be evaluated and justified if necessary. These reports should include sections dealing with methods of entry, interactions with employees of clients and third parties and other areas identified as potentially controversial. Consultants should be encouraged to take photographs and videos to further document their activities. Internal Audit should review samples of those records to establish whether sufficient evidence is being retained in the event that Saefwell has to defend the actions of its staff. For example, the broken window referred to in a complaint by a third party could leave Saefwell exposed to a claim, but it will be possible to minimise the cost of settling any such claim if a detailed record is available.

Strategic Level Case Study May 2024 – August 2024

Marking Guidance

Variant 1

About this marking scheme

This marking scheme has been prepared for the 2019 CGMA Professional Qualification Strategic Case Study [May and August 2024].

The indicative answers will show the expected or most orthodox approach; however, the nature of the case study examination tasks means that a range of responses will be valid. The descriptors within this level-based marking scheme are holistic and can accommodate a range of acceptable responses.

General marking guidance is given below, and markers are subject to extensive training, standardisation activities and ongoing monitoring to ensure that judgements are being made correctly and consistently.

Care must be taken not to make too many assumptions about future marking schemes on the basis of this document. While the guiding principles remain constant, details may change depending on the content of a particular case study examination form.

General marking guidance

- Marking schemes should be applied positively, with candidates rewarded for what they have demonstrated and not penalised for omissions.
- All marks on the scheme are designed to be awarded, and full marks should be awarded when all level descriptor criteria are met.

- The marking scheme and indicative answers are provided as a guide to markers. They are not intended to be exhaustive and other valid approaches must be rewarded. Equally, candidates do not have to make all of the points mentioned in the indicative answers to receive the highest level of the marking scheme.
- An answer which does not address the requirements of the task must be awarded no marks.
- Markers should mark according to the marking scheme and not their perception of where the passing standard may lie.
- Where markers are in doubt as to the application of the marking scheme to a particular candidate script, they must contact their lead marker.

How to use this levels-based marking scheme

1. Read the candidate's response in full

2. Select the level

- For each trait in the marking scheme, read each level descriptor and select one, using a best-fit approach.
- The response does not need to meet all of the criteria of the level descriptor – it should be placed at the level when it meets more of the criteria of this level than the criteria of the other levels.
- If the work fits more than one level, judge which one provides the best match.
- If the work is on the borderline between two levels, then it should be placed either at the top of the lower band or the bottom of the higher band, depending on where it fits best.

3. Select a mark within the level

- Once you have selected the level, you will need to choose the mark to apply.
- A small range of marks may be given at each level. You will need to use your professional judgement to decide which mark to allocate.
- If the answer is of high quality and convincingly meets the requirements of the level, then you should award the highest mark available. If not, then you should award a lower mark within the range available, making a judgement on the overall quality of the answer in relation to the level descriptor.

Summary of the core activities tested within each sub-task

Sub-task	Core activity		Sub-task weighting (% section time)
Section 1			
(a)	B	Evaluate business ecosystem and business environment	50%
(b)	D	Evaluate and mitigate risk	50%
Section 2			
(a)	E	Recommend and maintain a sound control environment	40%
(b)	C	Recommend financing strategies	60%
Section 3			
(a)	A	Develop business strategy	60%
(b)	E	Recommend and maintain a sound control environment	40%

SECTION 1			
Task (a) Identify and evaluate the needs of the stakeholders who will be affected by Saefwell's acceptance of this assignment.			
Trait			
1 st stakeholder	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies stakeholder	1-2
	Level 2	Evaluates stakeholder's needs	3-4
	Level 3	Evaluates stakeholder's needs with justification	5-6
2 nd stakeholder	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies stakeholder	1-2
	Level 2	Evaluates stakeholder's needs	3-4
	Level 3	Evaluates stakeholder's needs with justification	5-6
3 rd stakeholder	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies stakeholder	1
	Level 2	Evaluates stakeholder's needs	2-3
	Level 3	Evaluates stakeholder's needs with justification	4-5
Task (b) Identify and evaluate the ethical implications for Saefwell of accepting this assignment under the conditions set out by Wavhull's Non-Executive Chair.			
Trait			
1 st implication	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes ethical principle	1-2
	Level 2	Applies principle	3-4
	Level 3	Applies principle with justification	5-6

2 nd implication	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes ethical principle	1-2
	Level 2	Applies principle	3-4
	Level 3	Applies principle with justification	5-6
3 rd implication	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes ethical principle	1
	Level 2	Applies principle	2-3
	Level 3	Applies principle with justification	4-5

SECTION 2			
Task (a) Evaluate the arguments for and against having Saefwell's Internal Audit Department review the work done to date by the consultants before we decide whether to investigate further.			
Trait			
Arguments for	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies argument	1-2
	Level 2	Evaluates argument	3-4
	Level 3	Evaluates argument with justification	5-6
Arguments against	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies argument	1-2
	Level 2	Evaluates argument	3-4
	Level 3	Evaluates argument with justification	5-6
Task (b) Evaluate the likely impact on Saefwell's share price if the rumours concerning the true purpose of the Wavhull investigation are reported in the press.			
Trait			
1 st argument	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies argument relating to share price	1-2
	Level 2	Evaluates argument relating to share price	3-5
	Level 3	Evaluates argument relating to share price with justification	6-7
2 nd argument	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies argument relating to share price	1-2
	Level 2	Evaluates argument relating to share price	3-5
	Level 3	Evaluates argument relating to share price with justification	6-7
3 rd argument	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies argument relating to share price	1-2
	Level 2	Evaluates argument relating to share price	3-5
	Level 3	Evaluates argument relating to share price with justification	6-7

SECTION 3			
Task (a) Evaluate the arguments for and against Greg's belief that the acquisition of Laubooker would benefit the Saefwell Group.			
Trait			
1 st argument for	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies argument for acquisition	1-2
	Level 2	Evaluates argument for acquisition	3-4
	Level 3	Evaluates argument for acquisition with justification	5-6
2 nd argument for	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies argument for acquisition	1
	Level 2	Evaluates argument for acquisition	2-3
	Level 3	Evaluates argument for acquisition with justification	4-5
1 st argument against	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies argument against acquisition	1
	Level 2	Evaluates argument against acquisition	2-3
	Level 3	Evaluates argument against acquisition with justification	4-5
2 nd argument against	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies argument against acquisition	1
	Level 2	Evaluates argument against acquisition	2-3
	Level 3	Evaluates argument against acquisition with justification	4-5

Task (b) Identify and evaluate the post-acquisition issues that might have a negative impact on Saefwell's acquisition of Laubooker.			
Trait			
1st issue	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies issue	1
	Level 2	Evaluates issue	2-3
	Level 3	Evaluates issue with justification	4
2nd issue	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies issue	1
	Level 2	Evaluates issue	2-3
	Level 3	Evaluates issue with justification	4
3rd issue	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies issue	1
	Level 2	Evaluates issue	2-3
	Level 3	Evaluates issue with justification	4

Strategic Level Case Study May 2024 – August 2024

Marking Guidance

Variant 2

About this marking scheme

This marking scheme has been prepared for the 2019 CGMA Professional Qualification Strategic Case Study [May and August 2024].

The indicative answers will show the expected or most orthodox approach; however, the nature of the case study examination tasks means that a range of responses will be valid. The descriptors within this level-based marking scheme are holistic and can accommodate a range of acceptable responses.

General marking guidance is given below, and markers are subject to extensive training, standardisation activities and ongoing monitoring to ensure that judgements are being made correctly and consistently.

Care must be taken not to make too many assumptions about future marking schemes on the basis of this document. While the guiding principles remain constant, details may change depending on the content of a particular case study examination form.

General marking guidance

- Marking schemes should be applied positively, with candidates rewarded for what they have demonstrated and not penalised for omissions.
- All marks on the scheme are designed to be awarded, and full marks should be awarded when all level descriptor criteria are met.

- The marking scheme and indicative answers are provided as a guide to markers. They are not intended to be exhaustive and other valid approaches must be rewarded. Equally, candidates do not have to make all of the points mentioned in the indicative answers to receive the highest level of the marking scheme.
- An answer which does not address the requirements of the task must be awarded no marks.
- Markers should mark according to the marking scheme and not their perception of where the passing standard may lie.
- Where markers are in doubt as to the application of the marking scheme to a particular candidate script, they must contact their lead marker.

How to use this levels-based marking scheme

1. Read the candidate's response in full

2. Select the level

- For each trait in the marking scheme, read each level descriptor and select one, using a best-fit approach.
- The response does not need to meet all of the criteria of the level descriptor – it should be placed at the level when it meets more of the criteria of this level than the criteria of the other levels.
- If the work fits more than one level, judge which one provides the best match.
- If the work is on the borderline between two levels, then it should be placed either at the top of the lower band or the bottom of the higher band, depending on where it fits best.

3. Select a mark within the level

- Once you have selected the level, you will need to choose the mark to apply.
- A small range of marks may be given at each level. You will need to use your professional judgement to decide which mark to allocate.
- If the answer is of high quality and convincingly meets the requirements of the level, then you should award the highest mark available. If not, then you should award a lower mark within the range available, making a judgement on the overall quality of the answer in relation to the level descriptor.

Summary of the core activities tested within each sub-task

Sub-task	Core activity		Sub-task weighting (% section time)
Section 1			
(a)	C	Recommend financing strategies	50%
(b)	E	Recommend and maintain a sound control environment	50%
Section 2			
(a)	A	Develop business strategy	60%
(b)	B	Evaluate business ecosystem and business environment	40%
Section 3			
(a)	B	Evaluate business ecosystem and business environment	40%
(b)	D	Evaluate and mitigate risk	60%

SECTION 1			
Task (a) Evaluate the implications of the share price movements that have been observed for companies who have published annual reports both with and without volunteering the new disclosures on digital security.			
Trait			
1 st implication	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes implication	1-2
	Level 2	Evaluates implication	3-4
	Level 3	Evaluates implication with justification	5-6
2 nd implication	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes implication	1-2
	Level 2	Evaluates implication	3-4
	Level 3	Evaluates implication with justification	5-6
3 rd implication	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes implication	1
	Level 2	Evaluates implication	2-3
	Level 3	Evaluates implication with justification	4-5
Task (b) Identify and evaluate the governance issues that are associated with managing digital security risks and recommend with reasons how Saefwell might manage those issues.			
Trait			
Identification	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies issues	1-3
	Level 2	Evaluates issues	4-6
	Level 3	Evaluates issues with justification	7-9
Recommendation	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Suggests responses	1-2
	Level 2	Recommends responses	3-5
	Level 3	Recommends responses with justification	6-8

SECTION 2			
Task (a) Evaluate the opportunities and threats to the Saefwell Group assuming that it acquires Ilnbyte in order to cope with the demand for professional services arising from the requirement to disclose digital security risks.			
Trait			
Opportunities	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies opportunities	1-3
	Level 2	Evaluates opportunities	4-7
	Level 3	Evaluates opportunities with justification	8-11
Threats	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies threats	1-3
	Level 2	Evaluates threats	4-7
	Level 3	Evaluates opportunities with threats	8-10
Task (b) Recommend with reasons the approach that Saefwell should take to the evaluation and management of the currency risks arising from ownership of Ilnbyte.			
Trait			
1 st recommendation	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes response	1
	Level 2	Relates recommendation to risk	2-3
	Level 3	Offers good justification for recommendation	4
2 nd recommendation	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes response	1
	Level 2	Relates recommendation to risk	2-3
	Level 3	Offers good justification for recommendation	4
3 rd recommendation	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes response	1
	Level 2	Relates recommendation to risk	2-3
	Level 3	Offers good justification for recommendation	4

SECTION 3			
Task (a) Recommend with reasons the manner in which quoted companies might report their performance in order to reassure stakeholders that they are committed to the proper management of digital security.			
Trait			
1 st approach	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes issue	1
	Level 2	Recommends approach	2-3
	Level 3	Recommends approach with justification	4
2 nd approach	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes issue	1
	Level 2	Recommends approach	2-3
	Level 3	Recommends approach with justification	4
3 rd approach	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes issue	1
	Level 2	Recommends approach	2-3
	Level 3	Recommends approach with justification	4
Task (b) Evaluate the ethical arguments for and against omitting “trivial” incidents from the report on digital security.			
Trait			
1 st ethical argument	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes ethical issue	1-2
	Level 2	Evaluates argument	3-4
	Level 3	Evaluates argument with good justification	5-6
2 nd ethical argument	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes ethical issue	1
	Level 2	Evaluates argument	2-3
	Level 3	Evaluates argument with good justification	4-5
	Level	Descriptor	Marks

3 rd ethical argument		No rewardable material	0
	Level 1	Describes ethical issue	1
	Level 2	Evaluates argument	2-3
	Level 3	Evaluates argument with good justification	4-5
4 th ethical argument	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes ethical issue	1
	Level 2	Evaluates argument	2-3
	Level 3	Evaluates argument with good justification	4-5

Strategic Level Case Study May – August 2024

Marking Guidance

Variant 3

About this marking scheme

This marking scheme has been prepared for the 2019 CGMA Professional Qualification Strategic Case Study [May and August 2024].

The indicative answers will show the expected or most orthodox approach; however, the nature of the case study examination tasks means that a range of responses will be valid. The descriptors within this level-based marking scheme are holistic and can accommodate a range of acceptable responses.

General marking guidance is given below, and markers are subject to extensive training, standardisation activities and ongoing monitoring to ensure that judgements are being made correctly and consistently.

Care must be taken not to make too many assumptions about future marking schemes on the basis of this document. While the guiding principles remain constant, details may change depending on the content of a particular case study examination form.

General marking guidance

- Marking schemes should be applied positively, with candidates rewarded for what they have demonstrated and not penalised for omissions.
- All marks on the scheme are designed to be awarded, and full marks should be awarded when all level descriptor criteria are met.

- The marking scheme and indicative answers are provided as a guide to markers. They are not intended to be exhaustive and other valid approaches must be rewarded. Equally, candidates do not have to make all of the points mentioned in the indicative answers to receive the highest level of the marking scheme.
- An answer which does not address the requirements of the task must be awarded no marks.
- Markers should mark according to the marking scheme and not their perception of where the passing standard may lie.
- Where markers are in doubt as to the application of the marking scheme to a particular candidate script, they must contact their lead marker.

How to use this levels-based marking scheme

1. Read the candidate's response in full

2. Select the level

- For each trait in the marking scheme, read each level descriptor and select one, using a best-fit approach.
- The response does not need to meet all of the criteria of the level descriptor – it should be placed at the level when it meets more of the criteria of this level than the criteria of the other levels.
- If the work fits more than one level, judge which one provides the best match.
- If the work is on the borderline between two levels, then it should be placed either at the top of the lower band or the bottom of the higher band, depending on where it fits best.

3. Select a mark within the level

- Once you have selected the level, you will need to choose the mark to apply.
- A small range of marks may be given at each level. You will need to use your professional judgement to decide which mark to allocate.
- If the answer is of high quality and convincingly meets the requirements of the level, then you should award the highest mark available. If not, then you should award a lower mark within the range available, making a judgement on the overall quality of the answer in relation to the level descriptor.

Summary of the core activities tested within each sub-task

Sub-task	Core activity		Sub-task weighting (% section time)
Section 1			
(a)	B	Evaluate business ecosystem and business environment	50%
(b)	A	Develop business strategy	50%
Section 2			
(a)	C	Recommend financing strategies	60%
(b)	D	Evaluate and mitigate risk	40%
Section 3			
(a)	D	Evaluate and mitigate risk	40%
(b)	E	Recommend and maintain a sound control environment	60%

SECTION 1			
Task (a) Evaluate the political risks that this event might create for Saefwell in relation to its operations in Neerland.			
Trait			
1 st risk	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes risk	1-2
	Level 2	Evaluates risk	3-4
	Level 3	Evaluates risk with justification	5-6
2 nd risk	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes risk	1-2
	Level 2	Evaluates risk	3-4
	Level 3	Evaluates risk with justification	5-6
3 rd risk	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes risk	1
	Level 2	Evaluates risk	2-3
	Level 3	Evaluates risk with justification	4-5
Task (b) Recommend with reasons whether Saefwell should adopt an emergent approach to the development of strategies for providing clients with physical security services.			
Trait			
1 st argument	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes issue	1-2
	Level 2	Makes recommendation relating to issue	3-4
	Level 3	Makes recommendation relating to issue with justification	5-6
2 nd argument	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes issue	1-2
	Level 2	Makes recommendation relating to issue	3-4
3 rd argument	Level 3	Makes recommendation relating to issue with justification	5-6
	Level	Descriptor	Marks

		No rewardable material	0
	Level 1	Describes issue	1
	Level 2	Makes recommendation relating to issue	2-3
	Level 3	Makes recommendation relating to issue with justification	4-5

SECTION 2			
Task (a) Evaluate whether the significant decrease in Saefwell's share price is inconsistent with the facts that the company has not announced its intentions with respect to its widespread use of security cameras and the company's low beta coefficient.			
Trait			
Announcement of intentions (1)	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies issues	1-2
	Level 2	Evaluates arguments	3-4
	Level 3	Evaluates arguments with justification	5-6
Announcement of intentions (2)	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies issues	1
	Level 2	Evaluates arguments	2-3
	Level 3	Evaluates arguments with justification	4-5
Low beta coefficient (1)	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies issues	1
	Level 2	Evaluates arguments	2-3
	Level 3	Evaluates arguments with justification	4-5
Low beta coefficient (2)	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies issues	1
	Level 2	Evaluates arguments	2-3
	Level 3	Evaluates arguments with justification	4-5

Task (b) Evaluate the argument that Saefwell's Board should have foreseen the negative publicity relating to the manner in which it uses security cameras.			
Trait			
1 st argument	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes argument	1
	Level 2	Evaluates argument	2-3
	Level 3	Evaluates argument with justification	4
2 nd argument	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes argument	1
	Level 2	Evaluates argument	2-3
	Level 3	Evaluates argument with justification	4
3 rd argument	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes argument	1
	Level 2	Evaluates argument	2-3
	Level 3	Evaluates argument with justification	4

SECTION 3			
Task (a) Evaluate the ethical issues arising from Bai Jing's argument that Saefwell should continue to use security cameras as before, despite the fact that it is in breach of local laws in some cases.			
Trait			
1 st ethical issue	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes ethical issue	1
	Level 2	Evaluates ethical issue	2-3
	Level 3	Evaluates ethical issue with justification	4
2 nd ethical issue	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes ethical issue	1
	Level 2	Evaluates ethical issue	2-3
	Level 3	Evaluates ethical issue with justification	4
3 rd ethical issue	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes ethical issue	1
	Level 2	Evaluates ethical issue	2-3
	Level 3	Evaluates ethical issue with justification	4
Task (b) Recommend with reasons how Saefwell's Internal Audit Department might ensure that staff training and new procedures will be effective in ensuring that security staff assigned to vulnerable access points are safe.			
Trait			
1 st review	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes work done by internal audit	1-2
	Level 2	Describes work done in detail	3-4
	Level 3	Describes work done in detail with explanation	5-6
2 nd review	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes work done by internal audit	1
	Level 2	Describes work done in detail	2-3
	Level 3	Describes work done in detail with explanation	4-5

3rd review	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes work done by internal audit	1
	Level 2	Describes work done in detail	2-3
	Level 3	Describes work done in detail with explanation	4-5
4th review	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes work done by internal audit	1
	Level 2	Describes work done in detail	2-3
	Level 3	Describes work done in detail with explanation	4-5

Strategic Level Case Study May – August 2024

Marking Guidance

Variant 4

About this marking scheme

This marking scheme has been prepared for the 2019 CGMA Professional Qualification Strategic Case Study [May & August 2024].

The indicative answers will show the expected or most orthodox approach; however, the nature of the case study examination tasks means that a range of responses will be valid. The descriptors within this level-based marking scheme are holistic and can accommodate a range of acceptable responses.

General marking guidance is given below, and markers are subject to extensive training, standardisation activities and ongoing monitoring to ensure that judgements are being made correctly and consistently.

Care must be taken not to make too many assumptions about future marking schemes on the basis of this document. While the guiding principles remain constant, details may change depending on the content of a particular case study examination form.

General marking guidance

- Marking schemes should be applied positively, with candidates rewarded for what they have demonstrated and not penalised for omissions.
- All marks on the scheme are designed to be awarded, and full marks should be awarded when all level descriptor criteria are met.

- The marking scheme and indicative answers are provided as a guide to markers. They are not intended to be exhaustive and other valid approaches must be rewarded. Equally, candidates do not have to make all of the points mentioned in the indicative answers to receive the highest level of the marking scheme.
- An answer which does not address the requirements of the task must be awarded no marks.
- Markers should mark according to the marking scheme and not their perception of where the passing standard may lie.
- Where markers are in doubt as to the application of the marking scheme to a particular candidate script, they must contact their lead marker.

How to use this levels-based marking scheme

1. Read the candidate's response in full

2. Select the level

- For each trait in the marking scheme, read each level descriptor and select one, using a best-fit approach.
- The response does not need to meet all of the criteria of the level descriptor – it should be placed at the level when it meets more of the criteria of this level than the criteria of the other levels.
- If the work fits more than one level, judge which one provides the best match.
- If the work is on the borderline between two levels, then it should be placed either at the top of the lower band or the bottom of the higher band, depending on where it fits best.

3. Select a mark within the level

- Once you have selected the level, you will need to choose the mark to apply.
- A small range of marks may be given at each level. You will need to use your professional judgement to decide which mark to allocate.
- If the answer is of high quality and convincingly meets the requirements of the level, then you should award the highest mark available. If not, then you should award a lower mark within the range available, making a judgement on the overall quality of the answer in relation to the level descriptor.

Summary of the core activities tested within each sub-task

Sub-task	Core activity		Sub-task weighting (% section time)
Section 1			
(a)	A	Develop business strategy	60%
(b)	B	Evaluate business ecosystem and business environment	40%
Section 2			
(a)	B	Evaluate business ecosystem and business environment	40%
(b)	C	Recommend financing strategies	60%
Section 3			
(a)	D	Evaluate and mitigate risk	50%
(b)	E	Recommend and maintain a sound control environment	50%

SECTION 1			
Task (a) Evaluate the arguments for and against treating Saefwell's cyber security as a strategic matter that should be managed by the Board.			
Trait			
1 st argument for	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an argument	1-2
	Level 2	Evaluates the argument	3-4
	Level 3	Evaluates the argument with justification	5-6
2 nd argument for	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an argument	1
	Level 2	Evaluates the argument	2-3
	Level 3	Evaluates the argument with justification	4-5
1 st argument against	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an argument	1
	Level 2	Evaluates the argument	2-3
	Level 3	Evaluates the argument with justification	4-5
2 nd argument against	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an argument	1
	Level 2	Evaluates the argument	2-3
	Level 3	Evaluates the argument with justification	4-5

Task (b) Recommend with reasons the key performance indicators (KPIs) that the Internal Security Department might submit to the Board.			
Trait			
1 st KPI	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies a KPI	1
	Level 2	Explains the KPI	2-3
	Level 3	Justifies the KPI	4
2 nd KPI	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies a KPI	1
	Level 2	Explains the KPI	2-3
	Level 3	Justifies the KPI	4
3 rd KPI	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies a KPI	1
	Level 2	Explains the KPI	2-3
	Level 3	Justifies the KPI	4

SECTION 2			
Task (a) Identify and evaluate the power and interest of key stakeholder groups who are affected by this news report and the actions that Saefwell might take to manage its relationship with those stakeholders.			
Trait			
1 st stakeholder	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies stakeholder	1
	Level 2	Discusses stakeholder power and interest	2-3
	Level 3	Discusses stakeholder power and interest with justification	4
2 nd stakeholder	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies stakeholder	1
	Level 2	Discusses stakeholder power and interest	2-3
	Level 3	Discusses stakeholder power and interest with justification	4
3 rd stakeholder	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies stakeholder	1
	Level 2	Discusses stakeholder power and interest	2-3
	Level 3	Discusses stakeholder power and interest with justification	4
Task (b) Recommend with reasons the actions that Saefwell's Board should take in order to protect the company's share price.			
Trait			
1 st priority	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an issue	1-2
	Level 2	Recommends a response	3-4
	Level 3	Recommends a response with justification	5-6
2 nd priority	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an issue	1
	Level 2	Recommends a response	2-3
	Level 3	Recommends a response with justification	4-5

3 rd priority	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an issue	1
	Level 2	Recommends a response	2-3
	Level 3	Recommends a response with justification	4-5
4 th priority	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an issue	1
	Level 2	Recommends a response	2-3
	Level 3	Recommends a response with justification	4-5

SECTION 3			
Task (a) Evaluate the argument that Saefwell's Board should have managed the acquisition of Mowrtron differently.			
Trait			
1 st issue	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies a management issue	1-2
	Level 2	Evaluates the management issue	3-4
	Level 3	Evaluates the management issue with justification	5-6
2 nd issue	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies a management issue	1-2
	Level 2	Evaluates the management issue	3-4
	Level 3	Evaluates the management issue with justification	5-6
3 rd issue	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies a management issue	1
	Level 2	Evaluates the management issue	2-3
	Level 3	Evaluates the management issue with justification	4-5
Task (b) Evaluate the ethical implications of Saefwell's Board remaining silent about the loss of consultants from Mowrtron.			
Trait			
1 st implication	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an implication	1-2
	Level 2	Evaluates the implication	3-4
	Level 3	Evaluates the implication with justification	5-6
2 nd implication	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an implication	1-2
	Level 2	Evaluates the implication	3-4
3 rd implication	Level 3	Evaluates the implication with justification	5-6
	Level	Descriptor	Marks

		No rewardable material	0
	Level 1	Identifies an implication	1
	Level 2	Evaluates the implication	2-3
	Level 3	Evaluates the implication with justification	4-5

Strategic Level Case Study May – August 2024

Marking Guidance

Variant 5

About this marking scheme

This marking scheme has been prepared for the 2019 CGMA Professional Qualification Strategic Case Study [May & August 2024].

The indicative answers will show the expected or most orthodox approach; however, the nature of the case study examination tasks means that a range of responses will be valid. The descriptors within this level-based marking scheme are holistic and can accommodate a range of acceptable responses.

General marking guidance is given below, and markers are subject to extensive training, standardisation activities and ongoing monitoring to ensure that judgements are being made correctly and consistently.

Care must be taken not to make too many assumptions about future marking schemes on the basis of this document. While the guiding principles remain constant, details may change depending on the content of a particular case study examination form.

General marking guidance

- Marking schemes should be applied positively, with candidates rewarded for what they have demonstrated and not penalised for omissions.
- All marks on the scheme are designed to be awarded, and full marks should be awarded when all level descriptor criteria are met.

- The marking scheme and indicative answers are provided as a guide to markers. They are not intended to be exhaustive and other valid approaches must be rewarded. Equally, candidates do not have to make all of the points mentioned in the indicative answers to receive the highest level of the marking scheme.
- An answer which does not address the requirements of the task must be awarded no marks.
- Markers should mark according to the marking scheme and not their perception of where the passing standard may lie.
- Where markers are in doubt as to the application of the marking scheme to a particular candidate script, they must contact their lead marker.

How to use this levels-based marking scheme

1. Read the candidate's response in full

2. Select the level

- For each trait in the marking scheme, read each level descriptor and select one, using a best-fit approach.
- The response does not need to meet all of the criteria of the level descriptor – it should be placed at the level when it meets more of the criteria of this level than the criteria of the other levels.
- If the work fits more than one level, judge which one provides the best match.
- If the work is on the borderline between two levels, then it should be placed either at the top of the lower band or the bottom of the higher band, depending on where it fits best.

3. Select a mark within the level

- Once you have selected the level, you will need to choose the mark to apply.
- A small range of marks may be given at each level. You will need to use your professional judgement to decide which mark to allocate.
- If the answer is of high quality and convincingly meets the requirements of the level, then you should award the highest mark available. If not, then you should award a lower mark within the range available, making a judgement on the overall quality of the answer in relation to the level descriptor.

Summary of the core activities tested within each sub task

Sub-task	Core activity		Sub-task weighting (% section time)
Section 1			
(a)	A	Develop a business strategy	60%
(b)	B	Evaluate business ecosystem and business environment	40%
Section 2			
(a)	B	Evaluate business ecosystem and business environment	40%
(b)	C	Recommend financing strategies	60%
Section 3			
(a)	D	Evaluate and mitigate risk	50%
(b)	E	Recommend and maintain a sound control environment	50%

SECTION 1			
Task (a) Using scenario planning thinking, discuss how each of the following possibilities associated with our employment of cyber security experts from the police and military might apply to Saefwell.			
Trait			
Matching salaries	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies issues	1-2
	Level 2	Evaluates the scenario	3-5
	Level 3	Responds to the scenario	6-7
Ten-year enlistment	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies issues	1-2
	Level 2	Evaluates the scenario	3-5
	Level 3	Responds to the scenario	6-7
Legislation	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies issues	1-2
	Level 2	Evaluates the scenario	3-5
	Level 3	Responds to the scenario	6-7
Task (b) Evaluate the political risks associated with doing business in countries from which we recruit cyber security experts from the police and military.			
Trait			
1 st risk	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies a risk	1
	Level 2	Evaluates the risk	2-3
	Level 3	Evaluates the risk with justification	4
2 nd risk	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies a risk	1
	Level 2	Evaluates the risk	2-3
	Level 3	Evaluates the risk with justification	4

3 rd risk	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies a risk	1
	Level 2	Evaluates the risk	2-3
	Level 3	Evaluates the risk with justification	4

SECTION 2			
Task (a) Identify and evaluate the power and interest of two key stakeholders (other than shareholders) who would be affected if Saefwell implemented Murat's proposal to offer cyber security services to Barrland's Police Service and recommend with reasons how those stakeholders' interests should be managed.			
Trait			
1 st stakeholder	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies a stakeholder	1-2
	Level 2	Discusses the interest	3-4
	Level 3	Offers a response to needs, with justification	5-6
2 nd stakeholder	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies a stakeholder	1-2
	Level 2	Discusses the interest	3-4
	Level 3	Offers a response to needs, with justification	5-6
Task (b) Identify and evaluate the implications of suspending Saefwell's dividend in order to finance this new venture.			
Trait			
1 st implication	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an implication	1-2
	Level 2	Evaluates the implication	3-4
	Level 3	Evaluates the implication with justification	5-6
2 nd implication	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an implication	1
	Level 2	Evaluates the implication	2-3
	Level 3	Evaluates the implication with justification	4-5

3 rd implication	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an implication	1
	Level 2	Evaluates the implication	2-3
	Level 3	Evaluates the implication with justification	4-5
4 th implication	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an implication	1
	Level 2	Evaluates the implication	2-3
	Level 3	Evaluates the implication with justification	4-5

SECTION 3			
Task (a) Recommend with reasons controls that might prevent a recurrence of these errors when checking candidates' backgrounds.			
Trait			
1 st control	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an issue	1-2
	Level 2	Recommends a control	3-4
	Level 3	Recommends a control with justification	5-6
2 nd control	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an issue	1-2
	Level 2	Recommends a control	3-4
	Level 3	Recommends a control with justification	5-6
3 rd control	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an issue	1
	Level 2	Recommends a control	2-3
	Level 3	Recommends a control with justification	4-5
Task (b) Evaluate the arguments for and against having Saefwell's Internal Audit Department perform background checks on candidates who are being considered for employment on the Police Service contract.			
Trait			
Arguments for	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes arguments	1-3
	Level 2	Discusses arguments	4-6
	Level 3	Discusses arguments with good justification	7-9
Arguments against	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes arguments	1-2
	Level 2	Discusses arguments	3-5
	Level 3	Discusses arguments with good justification	6-8

Strategic Level Case Study May – August 2024

Marking Guidance

Variant 6

About this marking scheme

This marking scheme has been prepared for the 2019 CGMA Professional Qualification Strategic Case Study [May 2024 & August 2024].

The indicative answers will show the expected or most orthodox approach; however, the nature of the case study examination tasks means that a range of responses will be valid. The descriptors within this level-based marking scheme are holistic and can accommodate a range of acceptable responses.

General marking guidance is given below, and markers are subject to extensive training, standardisation activities and ongoing monitoring to ensure that judgements are being made correctly and consistently.

Care must be taken not to make too many assumptions about future marking schemes on the basis of this document. While the guiding principles remain constant, details may change depending on the content of a particular case study examination form.

General marking guidance

- Marking schemes should be applied positively, with candidates rewarded for what they have demonstrated and not penalised for omissions.
- All marks on the scheme are designed to be awarded, and full marks should be awarded when all level descriptor criteria are met.

- The marking scheme and indicative answers are provided as a guide to markers. They are not intended to be exhaustive and other valid approaches must be rewarded. Equally, candidates do not have to make all of the points mentioned in the indicative answers to receive the highest level of the marking scheme.
- An answer which does not address the requirements of the task must be awarded no marks.
- Markers should mark according to the marking scheme and not their perception of where the passing standard may lie.
- Where markers are in doubt as to the application of the marking scheme to a particular candidate script, they must contact their lead marker.

How to use this levels-based marking scheme

1. Read the candidate's response in full

2. Select the level

- For each trait in the marking scheme, read each level descriptor and select one, using a best-fit approach.
- The response does not need to meet all of the criteria of the level descriptor – it should be placed at the level when it meets more of the criteria of this level than the criteria of the other levels.
- If the work fits more than one level, judge which one provides the best match.
- If the work is on the borderline between two levels, then it should be placed either at the top of the lower band or the bottom of the higher band, depending on where it fits best.

3. Select a mark within the level

- Once you have selected the level, you will need to choose the mark to apply.
- A small range of marks may be given at each level. You will need to use your professional judgement to decide which mark to allocate.
- If the answer is of high quality and convincingly meets the requirements of the level, then you should award the highest mark available. If not, then you should award a lower mark within the range available, making a judgement on the overall quality of the answer in relation to the level descriptor.

Summary of the core activities tested within each sub-task

Sub-task	Core activity		Sub-task weighting (% section time)
Section 1			
(a)	B	Evaluate business ecosystem and business environment	60%
(b)	D	Evaluate and mitigate risk	40%
Section 2			
(a)	A	Develop a business strategy	50%
(b)	C	Recommend financing strategies	50%
Section 3			
(a)	D	Evaluate and mitigate risk	40%
(b)	E	Recommend and maintain a sound control environment	60%

SECTION 1			
Task (a) Evaluate Bai Jing's proposal in terms of the suitability, feasibility and acceptability (SAF) criteria.			
Trait			
Suitability	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies criterion in context	1-2
	Level 2	Discusses criterion	3-5
	Level 3	Discusses criterion with justification	6-7
Feasibility	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies criterion in context	1-2
	Level 2	Discusses criterion	3-5
	Level 3	Discusses criterion with justification	6-7
Acceptability	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies criterion in context	1-2
	Level 2	Discusses criterion	3-5
	Level 3	Discusses criterion with justification	6-7
Task (b) Identify and evaluate the risks that this type of physical penetration testing could create for Saefwell's consultants.			
Trait			
1 st risk	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies a risk	1-2
	Level 2	Evaluates the risk	3-4
	Level 3	Evaluates the risk with justification	5-6
2 nd risk	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies a risk	1-2
	Level 2	Evaluates the risk	3-4
	Level 3	Evaluates the risk with justification	5-6

SECTION 2			
Task (a) Evaluate the arguments for and against the acquisition of Sneektheef as opposed to Saefwell creating its own physical penetration testing business.			
Trait			
Arguments for	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an argument	1-3
	Level 2	Evaluates the argument	4-6
	Level 3	Evaluates the argument with justification	7-9
Arguments against	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies an argument	1-2
	Level 2	Evaluates the argument	3-5
	Level 3	Evaluates the argument with justification	6-8
Task (b) Identify and evaluate the challenges associated with negotiating the exchange of shares with Sneektheef's founder.			
Trait			
1 st challenge	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies a challenge	1-2
	Level 2	Evaluates the challenge	3-4
	Level 3	Evaluates the challenge with justification	5-6
2 nd challenge	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies a challenge	1-2
	Level 2	Evaluates the challenge	3-4
	Level 3	Evaluates the challenge with justification	5-6
3 rd challenge	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Identifies a challenge	1
	Level 2	Evaluates the challenge	2-3
	Level 3	Evaluates the challenge with justification	4-5

SECTION 3			
Task (a) Recommend with reasons how Saefwell could report its training programme as intellectual capital and human capital. Your recommendation should ignore the issues arising from the two incidents.			
Trait			
Intellectual capital	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes capital	1-2
	Level 2	Recommends reporting	3-4
	Level 3	Recommends reporting with justification	5-6
Human capital	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes capital	1-2
	Level 2	Recommends reporting	3-4
	Level 3	Recommends reporting with justification	5-6
Task (b) Recommend with reasons the work that Saefwell's Internal Audit Department might undertake in order to ensure that Saefwell's staff are not breaking the law when they undertake penetration testing assignments.			
Trait			
1 st recommendation	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes an audit objective	1-2
	Level 2	Recommends audit work	3-4
	Level 3	Recommends audit work with justification	5-6
2 nd recommendation	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes an audit objective	1
	Level 2	Recommends audit work	2-3
	Level 3	Recommends audit work with justification	4-5
3 rd recommendation	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes an audit objective	1
	Level 2	Recommends audit work	2-3
	Level 3	Recommends audit work with justification	4-5

4 th recommendation	Level	Descriptor	Marks
		No rewardable material	0
	Level 1	Describes an audit objective	1
	Level 2	Recommends audit work	2-3
	Level 3	Recommends audit work with justification	4-5

Strategic Level Case Study – Examiner’s report

May - August 2024 exam session

This document should be read in conjunction with the examiner’s suggested answers and marking guidance.

General comments

The Strategic case study (SCS) examinations for May and August 2024 were based on a pre-seen scenario which provided information about Saefwell, a quoted company that offers security services to its clients.

Saefwell offers both physical security and intelligence-led consultancy. Saefwell’s senior management must manage both the risks faced by the company itself and those faced by its clients. For example, a client might require advice about the mitigation of a security problem, dealing with which could create physical or reputational risks for Saefwell.

A total of six variants were set on Saefwell. The focus for each variant was as follows:

- Variant 1: Saefwell has been asked to investigate a dishonest director under conditions of secrecy that require the investigators to lie about the purpose of their assignment.
- Variant 2: Proposed changes to governance regulations concerning cyber risk may create opportunities for Saefwell.
- Variant 3: Saefwell staff assigned to secure property could be at physical risk.
- Variant 4: Saefwell is a prominent target for security breaches.
- Variant 5: Saefwell faces reputational risk because it is recruiting specialists from the police and military who have been trained by the government at great expense.
- Variant 6: A potential acquisition has been identified.

All six variants complied with the published blueprint and covered the core activities in the prescribed weightings. Each variant consisted of three tasks and each task was further subdivided into separate requirements. The weighting attached to each requirement was stated and candidates were advised to allocate the time available for each requirement on the basis of those weightings. Markers were instructed to adopt a holistic approach to marking, which meant that the answer to each requirement was

read and judged on its merits. Markers were provided with specific guidance as to the characteristics of level 1, level 2 and level 3 answers for each separate requirement.

As always, the key to achieving a passing mark or better is to answer the question as set. Failure to do so is one of the main reasons candidates fail the case study. Read the questions and the scene-setting pages carefully before attempting the questions. It is also vital that the candidates understand the pre-seen material. Candidates should apply their judgement to answering the requirements as fully as possible. Scenario-based questions often allow scope for differences of opinion and markers are instructed to mark different approaches on their merits.

To achieve a level 3 in most traits, it was expected that a candidate would demonstrate good technical understanding of the topic being tested through clear and logical application to the circumstances described in the scenario. It may also help to develop an argument by offering justification for any recommendations made. One way to formulate an answer to a typical requirement would be to imagine it as a task that had been set by a director who was delegating an important task. At strategic level, it is expected that there will be evidence of strategic thinking; this was not really demonstrated by candidates in the answers to this case study.

Level 1 answers generally demonstrate either poor exam technique or fail to offer a logical response to the circumstances in the scenario (or both). Poor exam technique is generally due to a failure to answer the question. Poor logic generally suggests that the candidate has misunderstood the scenario. For example, the specific issues arising in the case of Saefwell include:

- No two assignments are the same. Each must be planned and executed in its own way.
- Senior management must be aware of the risks facing Saefwell, which can often be affected by the risks faced by clients.
- The company faces risks that have very high impacts.

While each attribute may not necessarily inform every requirement, level 1 marks tended to be associated with a failure to appreciate the specifics of the business.

Variant 1 Comments on performance

	Designed to test	Core activity
Task 1	Saefwell has been asked to conduct a fraud investigation while lying about its true purpose. How will stakeholders be affected by accepting such an assignment?	B – Conduct an analysis of stakeholder needs and recommend appropriate responses.
	What are the ethical implications of accepting such an assignment?	D – Identify ethical dilemmas and recommend suitable responses.
Task 2	The investigation is well under way. There are concerns that the work should be reviewed by Saefwell's internal audit and that the press might publish rumours about the possible fraud. What are the arguments for and against involving internal audit?	E – Apply internal audit resources.
	What is the likely impact of publication of the rumours on Saefwell's share price?	C – Recommend and apply business valuation models.
Task 3	A consultancy that has specific skills in legal and accounting might be acquired. Would such an acquisition benefit Saefwell?	A – Evaluate potential acquisitions and divestment opportunities.
	What post-acquisition issues might arise?	E – Recommend responses to the threats arising from poor governance.

Task 1

Candidates were first asked to identify and evaluate the implications for the stakeholders of both Saefwell and Wayhull, who will be affected if Saefwell accepts this assignment.

Level 3 responses identified key stakeholders for both Saefwell and Wayhull and explained the implications for them. For example, Wayhull's shareholders will be affected because the investigation could impact their confidence in the Wayhull directors. Saefwell's shareholders would be interested because the assignment offers significant risks and rewards for the company. Level 2 responses also identified appropriate stakeholders and discussed the implications for them, but with less detailed evaluation. Some candidates

identified far too many stakeholders to be able to discuss the impact on them in any depth. Level 1 answers often went no further than identifying potentially relevant stakeholders without explanation.

Candidates were next asked to identify and evaluate the ethical implications for Saefwell of accepting this assignment under the pretence of conducting a risk assessment, as requested by Wayhull's Non-Executive Chair.

Level 3 responses identified and evaluated a range of ethical implications, such as the importance of confidentiality and the difficulty in complying fully with this, given that managers and staff at Wayhull could draw conclusions from the questions asked by consultants. The principle of integrity could be breached by the consultants being misleading about the purpose of the investigation. Objectivity would be difficult given that the consultants would be actively looking for incriminating evidence. Level 2 answers often focussed solely on the principle of integrity, concluding that the assignment should be refused unless its true purpose is revealed. Answers lacked depth of discussion and showed little evidence of strategic thinking. Level 1 responses often identified the CIMA ethical principles but did little to apply them to the scenario.

Task 2

In task 2, candidates were asked to evaluate the arguments for and against having Saefwell's Internal Audit Department review the work done to date by the consultants before deciding whether to investigate further.

Level 3 responses evaluated a number of arguments including the risk of reputational damage to Saefwell if the Chief Executive is offended by the investigation, the relevance of the skills of the Internal Audit Department and the danger of demotivating the consulting team. Arguments were well developed and explained in appropriate detail. Level 2 answers were often less well tailored to the specific scenario, making general points such as that the Internal Auditors would have appropriate skills but could be busy on other work, without focussing on scenario specific issues such as the risks to Saefwell and the nature of the checks which the Internal Audit Department could undertake. Level 1 answers identified some arguments but did not provide evaluation or any depth of discussion.

Candidates were next asked to evaluate the likely impact on Saefwell's share price if the rumours concerning the true purpose of the Wayhull investigation are reported in the press.

Level 3 responses identified and evaluated a number of relevant factors, such as the stock market's expectations of Saefwell's future cash flows, and the potential reputational damage to Saefwell if potential future clients are put off by the danger that their staff would be unsettled by Saefwell consultants who might not be carrying out the investigation they claim to be doing. They also recognised the upside potential that the market could regard the contract as positive news. Level 2 responses were less well developed and showed less sound understanding of how rumours could impact share price. Discussion was often too focussed on the damage which could

be done by Saefwell not revealing the real purpose of the investigation, without clearly explaining why this might be the case. Level 1 answers did not go further than identifying some issues.

Task 3

In task 3, candidates were asked to evaluate the arguments for and against Greg's belief that the acquisition of Laubooker would benefit the Saefwell Group.

Level 3 responses identified and evaluated a range of arguments both for and against the acquisition, such as the specialist service adding value to investigations and the additional expertise being attractive to potential clients, but also the downside that clients might not actually want to pursue legal action and Saefwell may not have sufficient demand to keep Laubooker's consultants occupied. Level 2 answers often lacked balance, presenting only arguments for or against and lacking the depth and detail needed to really evaluate the issues fully and demonstrate some strategic thinking. Level 1 answers identified a limited range of issues and did not develop their discussion fully.

The final task asked candidates to identify and evaluate the post-acquisition issues that might have a negative impact on Saefwell's acquisition of Laubooker.

Level 3 answers identified and evaluated a range of appropriate issues, such as the potential for conflict between the Laubooker founders and Saefwell Board, the risk that Laubooker's professional staff could choose to leave and the potential for differences in the professional obligations of each company's staff. Level 2 responses were less well developed and sometimes repeated issues from the first part of this task. Level 1 answers identified some potential issues but without evaluation; issues discussed were often generic rather than specific to the scenario presented by the case study.

Variant 2 Comments on performance

	Designed to test	Core activity
Task 1	New rules have been introduced in relation to disclosure of cyber risk. What are the implications of the apparent impact that voluntary disclosures have had on share prices?	C – Recommend and apply business valuation models.
	What are the governance issues associated with managing cyber risks?	E – Recommend responses to the threats arising from poor governance.
Task 2	These disclosures have been identified as a potential revenue source. Saefwell has identified a foreign consulting firm that might be a suitable acquisition. What are the opportunities and threats arising from this acquisition?	A – Recommend responses to opportunities and threats arising from digital technologies.
	What currency risks would arise from the acquisition of the consultancy?	B – Recommend responses to economic, political and currency risks.
Task 3	The reporting rules are under consideration. How might companies reassure their shareholders with regard to cyber risks?	B – Recommend KPIs that encourage sound strategic management.
	What are the ethical arguments for and against being selective in reporting incidents?	D – Identify ethical dilemmas and recommend suitable responses.

Task 1

The scenario opens with news that strict new disclosures regarding digital security will be required by the stock exchange. Candidates were requested to evaluate the implications of the share price movements that have been observed for companies who have published annual reports both with and without volunteering the new disclosures on digital security.

Level 3 responses gave a good discussion of the factors against a backdrop of market efficiency. Level 3 responses also tended to give a wide perspective of the issues, explaining that there could be a choice between taking short-term minor losses and longer-term recovery for companies who disclose the security issues against possible long-term damage to those who don't take the short-

term losses. Level 3 answers also often discussed the opportunity for Saefwell for further consultancy offerings to be made in the marketplace. Level 2 responses tended to focus on Saefwell only and not the wider market implications as requested, while level 1 responses were generally very one sided and restricted in their response.

In the second part of task 1, level 3 answers tended to get straight to strategy development at Board level, discussing whether restructuring and possible new appointments could be required. Good answers highlighted the random nature of the threat which can come from the exploitation of any weakness. Good answers highlighted that the expense encountered in mitigating possible threats is very difficult to justify as preventative actions are hard to quantify. However, significant benefits can accrue if these efforts can be promoted to the market as consultancy products. Level 2 responses tended to be more tactical, with some good generic answers but displaying less understanding of the risks. Level 1 answers generally were non-strategic and very generic.

There was a general lack of evidence of Strategic Board Governance in answers.

Task 2

In task 2, the scenario moves forward a month to consider the acquisition of a foreign digital consultancy group. Answers in this section were generally quite good with Level 3 responses highlighting the needs created by the disclosure changes and matching the Irnbyte skills to that need. Better candidates then highlighted and dealt with possible conflict with Irnbyte, critiquing previous consultancy work carried out by Saefwell. Level 2 answers tended to see only benefits and missed or ignored possible drawbacks whilst still giving reasonable coverage of benefits. Level 1 answers were generally vague and one sided and showed no strategic thinking.

In the second part of this task, candidates were requested to recommend with reasons the approach that Saefwell should take to the evaluation and management of the currency risks arising from ownership of Irnbyte.

There were a large proportion of very weak answers here. Good level 3 responses developed arguments about how best to assess the nature of the risk exposure in the first instance, looking at economic factors and checking historical volatility of the currencies against each other, then looking at the source of issues, salaries and running costs against revenues earned.

Evaluation of government stability and policies employed as part of the strategic view are also part of the overall evaluation techniques for currency stability and risk assessment. Once exposure can be assessed, then management techniques can be developed appropriate to the risk exposure. Level 2 answers were either less detailed in their approach or missed aspects of evaluation which were critical to understanding the problem to be managed. Level 1 answers tended to list a series of instruments without any real indication of how or when to apply them and usually had very limited awareness of the methods for evaluation of the risk.

Task 3

Level 3 responses gave good, structured answers dealing with strategic management, directed activity, assessing, training, protecting, testing, proactive readiness to respond and adapt to existing or developing threat. Level 2 answers were also good, though with less depth and often less emphasis on strategic board leadership being reported. Level 1 responses were weak and just listed everything they could think of whether relevant or not. Many candidates focussed entirely on the local Saefwell response rather than as requested “Quoted companies”.

Finally, candidates were asked to evaluate the ethical arguments for and against omitting “trivial” incidents from the report on digital security.

This was generally answered well, with much better treatment of ethics than has been seen in previous years. The main ethical issue here is professional behaviour which, of course, includes compliance with law and regulation which is the heart of this question. Confidentiality is also a key issue here, as respect has to be given to avoid accidental disclosure of potential attack areas while also assuring that all perimeters are secure. Good level 3 responses indicated that companies might provide definitions of what they consider relevant or trivial and thus above or below the reporting threshold. Level 2 answers were also good but tended to be less detailed. Level 1 answers tended to provide a list of ethics without much application to the scenario.

Variant 3 Comments on performance

	Designed to test	Core activity
Task 1	The government of a country in which Saefwell does business has banned the use of security cameras in public places. What political risks might arise from the continued use of cameras?	B – Recommend responses to economic, political and currency risks.
	Should Saefwell adopt an emergent approach to strategy development?	A – Recommend responses to opportunities and threats arising from digital technologies.
Task 2	The use of cameras has caused adverse publicity. Is the drop in share price consistent with the adverse publicity?	C – Recommend and apply business valuation models.
	Should Saefwell's Board have foreseen this adverse publicity?	D – Evaluate and mitigate cyber risks.
Task 3	A director is unhappy that the company has been asked to remove some cameras. New security procedures will have to be adopted. What are the ethical issues arising from the director's arguments?	D – Identify ethical dilemmas and recommend suitable responses.
	How might internal audit check compliance with the new security procedures?	E – Apply internal audit resources.

Task 1

Section 1 presented a news report, highlighting a recent complaint about Saefwell's operations in the country of Neerland.

This part of the task was answered well by most candidates, with many achieving a high level 2 or level 3 score. The strongest answers were focussed largely on the direct political risks that this complaint might cause. Many stronger answers also correctly discussed the problems of sanctions following the camera placement and recording. Level 3 and strong level 2 answers also considered the potential further risks that such penalties could cause, such as the reputational damage and the potential undermining of relationships with clients in Neerland. Weaker level 2 and level 1 answers were often poorly focussed on political risks, instead focussing only on a small number of other risks such as reputational and/or financial risks.

The second task in Section 1 was answered well by candidates that recognised that the nature of the security industry means that clients' needs and the environment in which those needs are to be met are constantly changing. Level 3 and strong level 2 answers recognised and discussed how an emergent approach to strategy formulation means that strategies can be updated in response to such changes. Level 3 and stronger level 2 responses also demonstrated strong application through considering how Saefwell could benefit from implementing an emergent strategy by taking a proactive approach to the threats that are emerging in the security industry and by approaching clients to offer options for addressing those threats.

Weaker level 2 and level 1 answers were often brief and largely theoretical, with many such answers only considering the differences between rational and emergent approaches to strategy.

Task 2

This question was generally not answered well, with only a small proportion of candidates scoring level 3 or high level 2 marks. Most candidates did present a reasonable discussion of the impact on the share price of Saefwell's lack of announcement of its intentions. The strongest answers provided a balanced assessment of the various factors potentially causing a fall in share price. However, for the second part of this task, very few candidates presented strong answers in relation to the impact of Saefwell's low beta coefficient. Many answers demonstrated poor understanding and application with many very brief responses, suggesting a lack of theoretical knowledge application to the circumstances of the case. Candidates who scored low level 2 or level 1 marks often presented answers which were wholly theoretical. For example, some candidates merely discussed in depth the Efficient Market Hypothesis with no direct application of this to the case context of the question. No marks are gained for pure theoretical knowledge with no direct application.

The second task in Section 2 was answered well by many candidates, with most presenting high level 2 responses. Level 3 and strong level 2 answers were well-balanced and clearly assessed whether or not the Board should have foreseen the negative publicity. Many stronger answers recognised that Saefwell has an executive director responsible for Legal, Risk and Business Ethics

and therefore that director's responsibilities should have included oversight of compliance with the law. Better answers also recognised that it could be considered unrealistic to expect the Board to review the security arrangements in place at individual clients' premises in sufficient detail to identify potential problems. Level 3 and higher level 2 answers were those that applied their answers directly to the case context and considered the role that the Director of Physical Security Services may have played in this situation.

Weaker level 2 and level 1 responses were often thin and not well balanced. Level 1 responses also sometimes focussed more on the structure and role of the Board members, rather than directly on the question that had been asked.

Task 3

The first task was answered well, with many candidates scoring a high level 2 or level 3 mark. Most candidates applied the five ethical principles to structure their responses, which often proved an effective approach. Level 3 and high strong level 2 answers were well applied to the case context and made good use of the reference material to support many of the points made. Although it was not necessary to apply all five ethical principles to score good marks, those that did were able to effectively and comprehensively consider the ethical issues arising from Bai's argument. Few candidates scored low level 2 or level 1 answers on this task, but those that did often presented answers that either failed to focus on the ethical issues relating to Bai's stance or were largely theoretical.

The second task in section 3 asked candidates to recommend with reasons how Saefwell's Internal Audit Department might ensure that staff training and new procedures will be effective in ensuring that security staff assigned to vulnerable access points are safe.

This question was generally not answered well, with very few candidates achieving a level 3 answer. Most answers showed little strategic thinking and could have been management level answers. There were some high level 2 responses which attempted to focus on how IA would assess the effectiveness of the training and new procedures required for security staff in vulnerable areas, although often answers strayed into activities that would in fact be carried out by the HR function. A significant proportion of answers to this task, however, were weaker level 2 responses, which often presented very generic or theoretical answers rather than being applied to the circumstances of the case, i.e. the specific IA activities required to ensure the effective training of staff assigned to vulnerable access points. Many lower level 2 and level 1 answers barely considered this at all.

Variant 4 Comments on performance

	Designed to test	Core activity
Task 1	Is it realistic to manage cyber security at a strategic level?	A – Recommend responses to opportunities and threats arising from digital technologies.
	What KPIs might Saefwell introduce to enable the Board to monitor performance?	B – Recommend KPIs that encourage sound strategic management.
Task 2	How should the Board respond to stakeholder needs in relation to this claim?	B – Conduct an analysis of stakeholder needs and recommend appropriate responses.
	What are the priorities for protecting Saefwell's share price?	C – Recommend and apply business valuation models.
Task 3	How should Saefwell's Board have handled the acquisition differently?	E – Recommend responses to the threats arising from poor governance.
	What are the ethical implications of remaining silent about the loss of staff?	D – Identify ethical dilemmas and recommend suitable responses.

Task 1

Saefwell is facing an increased number of attempts to breach the security of its network, and the company appears to be seen as an attractive target by potential intruders. This may be because the company's files include details of clients' security systems.

Candidates were first asked to evaluate the arguments for and against treating Saefwell's cyber security as a strategic matter that should be managed by the Board.

Level 3 responses identified arguments both for and against, such as the fact that oversight of internal controls is a Board responsibility, the need for Saefwell to protect its reputation by showing it is able to manage security threats but, on the other hand, the responsibilities of managers and staff tasked with managing cyber security threats. Arguments were well developed and clearly explained. Level 2 responses also identified appropriate arguments but did not fully evaluate or justify them. Level 1 answers often did not go beyond identifying issues, and some did not directly address the requirement, focussing on more general points about Saefwell's business model.

Candidates were next asked to recommend with reasons the key performance indicators (KPIs) that the Internal Security Department might submit to the Board.

Level 3 responses identified a limited number of relevant KPIs and gave a clear explanation justifying their choice. For example, logging instances when unauthorised parties successfully breached Saefwell's systems, details of staff training and updates to software systems would all be appropriate. Level 2 answers often provided a long list of KPIs but did not explain why they were appropriate. Some of these were not appropriate for the management of cyber security risks. Level 1 responses identified KPIs but provided no meaningful discussion or justification.

Task 2

Candidates were first asked to identify and evaluate the power and interest of key stakeholder groups (other than shareholders) who are affected by this news report and the actions that Saefwell might take to manage its relationship with those stakeholders.

Level 3 responses identified and discussed a limited number of stakeholder groups in some detail. Appropriate choices included clients, the police service, lenders, employees or members of the public. Evaluation of the power and interest of each stakeholder was well justified. Level 2 answers identified stakeholders but did not provide as much detailed discussion. Despite the question specifically excluding shareholders from the requirement, a number of candidates focussed on evaluating this group. Level 1 answers identified some appropriate stakeholders but did not expand their discussion beyond this.

Candidates were next asked to recommend with reasons the actions that Saefwell's Board should take in order to protect the company's share price.

Level 3 responses provided practical advice, identifying and prioritising actions. For example, it would be appropriate to begin with a rapid internal investigation to determine the extent of the breach, to appoint a public relations advisor and to communicate with key clients. Responses were discussed in detail and well justified. Level 2 answers discussed issues and responses but without detailed justification. Some were overly focussed on the efficient market hypothesis. Level 1 answers did not go further than identifying some issues and responses.

Task 3

In the final task, candidates were first asked to evaluate the arguments that Saefwell's Board should have managed the acquisition of Mowtron differently.

Level 3 responses gave a balance of arguments, recognising that the transition could have been smoother if Ramesh Kumar had stayed with the company for a period of time, that being honest about its plans for the consultants could have led to more of them staying with the company and that using a public relations consultant could have increased press attention. On the other hand, Saefwell did not intend to retain all the consultants and has saved redundancy costs due to them choosing to leave. Level 2 answers evaluated some issues but were less detailed and often one-sided. Level 1 responses identified issues correctly but did not explain them.

Finally, candidates were asked to evaluate the ethical implications of Saefwell's Board remaining silent about the loss of Mowtron consultants.

Level 3 answers identified and evaluated a range of appropriate ethical issues; for example, integrity in dealing with clients who will expect competent consultants to support their software and objectivity when answering questions about the retention of consultants. Level 2 answers often referenced the CIMA ethical framework but did not make good links between the ethical principles and the specific scenario. Level 1 answers correctly identified ethical principles but did not evaluate them.

Variant 5 Comments on performance

	Designed to test	Core activity
Task 1	How might scenario planning be used determine whether this approach to recruitment is sustainable?	A – Evaluate strategic options (digital and otherwise).
	How can the political risks of recruiting from overseas governments be managed?	B – Recommend responses to economic, political and currency risks.
Task 2	How should the needs of stakeholders be evaluated?	B – Conduct an analysis of stakeholder needs and recommend appropriate responses.
	What are the implications of suspending the dividend to finance this new venture?	C – Recommend suitable sources of finance.
Task 3	What controls should be introduced to prevent a recurrence?	D – Recommend internal controls.
	How might internal audit support HR in requirement in the future?	E – Apply internal audit resources.

Task 1

Security companies, including Saefwell, recruit large numbers of consultants from police and military services. That is putting those services under pressure to retain skilled staff.

The first sub-task asked for an evaluation of three possibilities that Saefwell might consider in the context of a scenario planning exercise. Each related to the broader issue of recruitment of consultants from the police and military. Level 3 answers offered potentially realistic outcomes of each of the scenarios. Those answers tended to reflect both the likelihood of a problem and the possibility that the possibilities might not arise. For example, there is a concern that the military will fund a year of full-time study in return for an additional 5-year commitment. Candidates at level 3 often pointed out the possibility that potential recruits might be reluctant to make such a commitment. Level 1 answers were often unrealistic and missed the point. For example, they pointed out that Saefwell could deal with the recruitment issue by delaying appointments for an additional 5 years.

The second sub-task asked about the political risks associated with doing business in countries from which Saefwell had recruited staff from the police and military. Level 3 answers were realistic, pointing out that the governments who had lost security staff to Saefwell might be inclined to retaliate in some manner, perhaps by imposing additional taxes or refusing to award government contracts for security work. Level 1 answers tended to be underdeveloped, with little real substance. They failed to identify the manner in which a government agency might respond to the loss of key staff.

Task 2

Saefwell plans to bid for cyber security work that Barrland's Police Service plans to outsource. That will require significant funding to be raised.

The first sub-task asked for an analysis of the power and interest of two key stakeholders, other than Saefwell's shareholders, who would be affected by this bid. A disturbing minority of candidates chose to evaluate the shareholders despite the instruction to the contrary. Level 3 answers tended to demonstrate good examination technique by selecting stakeholders who would be relatively easy to evaluate. They proceeded to offer a realistic assessment of the power and interest of those stakeholders. Level 1 answers tended to take a more haphazard approach to the selection of stakeholders and offered little justification for assertions about their level of power and interest.

The second sub-task dealt with the suspension of Saefwell's dividend in order to finance the expansion needed to support this bid. As is often the case for questions drawing on the F pillar, there was a wide range of answers. Level 3 answers focussed on the scenario, often with particular emphasis on the positive net present value that is likely to come from the investment in this project. Shareholders can benefit from the future cashflows that the assignment will generate. Candidates at this level also offered arguments relating to recent history of dividend payments and the company's current financial position. Level 1 answers tended to provide discussion based on study materials and failed to adapt the logic of that material to the scenario.

Task 3

Saefwell has recruited staff on the basis of false credentials relating to academic qualifications, prior experience and criminal records. It is important that these problems be addressed as a matter of some urgency.

The first sub-task asked for recommendations for controls that would address these problems. Level 3 answers distinguished themselves by offering clear recommendations with sufficient justification to indicate their effectiveness. It was possible to see whether such recommendations would address the problems. For example, requesting direct confirmation of academic qualifications from the institutions that granted the awards. Level 1 answers were often vague, making recommendations that qualifications should be checked, but with no indication of how that check might be conducted. Candidates also tended to suggest artificial intelligence as a possible response, with no indication as to how such software might be trained.

The second sub-task asked whether internal audit should carry out background checks on applicants. Level 3 answers generally provided a balanced argument, identifying both the potential contribution that internal audit might make to this activity and the disadvantages of redirecting internal audit resources. Level 1 answers tended to make unsupported assertions concerning the possible contribution that internal audit might make.

Variant 6 Comments on performance

	Designed to test	Core activity
Task 1	Would this meet the SAF criteria?	B – Select and apply suitable strategic analytical tools.
	What risks would this create for Saefwell's staff?	D – Evaluate risks and recommend responses and can maintain the corporate risk register.
Task 2	Would it be preferable to acquire the consultancy as a going concern?	A – Evaluate potential acquisitions and divestment opportunities.
	What are the challenges associated with negotiating a share for share exchange with the owner?	C – Recommend and apply business valuation models.
Task 3	Can the training be classified as enhancing non-financial capitals?	D – Identify ethical dilemmas and recommend suitable responses.
	How should internal audit ensure that staff are not being trained to break the laws in the various locations in which Saefwell operates?	E – Apply internal audit resources.

Task 1

The first task asked candidates to evaluate Bai Jing's proposal in terms of the suitability, feasibility and acceptability (SAF) criteria.

This part of the task was answered well by most candidates, with many achieving a high level 2 or level 3 score. The strongest answers were logical and well structured, presenting a range of applied points under each heading of the SAF criteria. Level 3 and strong level 2 answers were well applied to the case context and considered the reasons both for and against physical penetration systems being a viable strategy for Saefwell. This included consideration of the suitability with Saefwell's mission, vision and values, the reaction if its key stakeholders and the financial and human resources it has available. Weaker level 2 and level 1 answers were often poorly structured and failed to generate a sufficient range of applied evaluation points. Weaker answers also focussed incorrectly on assessing an acquisition of Sneektheef, which was not required. Candidates must be careful to read the requirements carefully and only focus on the question actually asked.

The second task answered well by those candidates that recognised that this task was focussing on the potential risks for Saefwell's consultants and not Saefwell itself as an organisation. Level 3 and strong level 2 answers recognised and discussed a range of

potential risks to consultants carrying out physical penetration testing, including physical attack, arrest and criminal charges, should they be discovered during an assignment. These responses also often demonstrated strong application through considering how Saefwell could potentially mitigate such threats through appropriate training and legal protection. Weaker level 2 and level 1 answers largely focussed on risks to Saefwell itself, such as legal, ethical and reputational risks of operating a physical penetration service. Some answers failed to consider risks to the consultant at all, which limited the score achieved. Again, candidates are reminded to ensure that they read the question requirements carefully.

Task 2

The first task asked candidates to evaluate the arguments for and against the acquisition of Sneektheef as opposed to creating a consultancy within Saefwell to offer a penetration testing service.

This question was reasonably well answered, with most candidates achieving a level 2 score or above. Most candidates did present a reasonable discussion of the arguments for and against an acquisition of Sneektheef and therefore obtained a higher level 2 mark, but few presented level 3 answers, which were those that also compared this to the pros and cons of Saefwell creating its own consultancy service. Stronger answers focussed on issues such as removing a competitor from the market as, although it would be possible for Saefwell to start up its own penetration testing business, it would then have to compete with Sneektheef for business and access to existing knowledge base relating to systems and procedures that might be difficult and time consuming to create independently. Stronger answers were well balanced in recognising the challenges such as lack of opportunity for Saefwell to check the backgrounds of the 150 consultants and the potential lack of detailed reports or financial information for a company like Sneektheef.

Weaker level 2 and level 1 answers were often very brief, and some candidates seemed to find it challenging to identify a suitable range of points. Some answers also lacked balance, considering only the reasons for or against the acquisition rather than both.

The second task in Section 2 asked candidates to identify and evaluate the challenges associated with negotiating the exchange of shares with Sneektheef's founder.

This question was answered reasonably well by many candidates, with most presenting high level 2 responses. Level 3 and strong level 2 answers were well focussed on the fact that Sneektheef is unquoted, which means that there is no objective valuation for the company. Better answers also recognised the need for clear and open negotiation. Stronger answers recognized that as an unquoted company, Sneektheef could be valued on comparatives relating to quoted companies, but recognized the difficulty in doing so as Sneektheef is a unique business that may not share the same systematic risk as any other.

Weaker level 2 and level 1 responses most often merely described several business valuation models with no real attempt to discuss their relevance or application to this business. Such answers were limited in not also considering issues such as negotiation and post-acquisition issues.

Task 3

This first task was answered well, with many candidates scoring a high level 2 mark. Most were able to recognise and discuss a range of ways in which the consultants and the additional training offered would add value to the two capitals identified. The better answers clearly distinguished between the two capitals, notably the intangible nature of intellectual capital. Weaker level 2 and level 1 answers tended to be more descriptive and failed to focus specifically on the added value impact of Sneektheef's consultant training. Some weaker candidates wasted time displaying general knowledge of the six capitals which was unnecessary and awarded very limited credit.

The second task in section 3 was generally not well answered, with few candidates achieving a level 3 score and few showing any strategic thinking. There were some high level 2 responses, which made a sound attempt to focus on activities that IA would need to focus on to ensure that consultants were not breaking the law. However, many answers often strayed into activities that would in fact be carried out by the HR function (such as designing training programs or recruitment activities).

However, a significant proportion of answers to this task were weaker level 2 responses, which often presented very generic or theoretical answers rather than being applied to the circumstances of the case, i.e. the specific IA activities required to ensure the effective training, management and supervision of staff assigned to physical penetration assignments and also to ensure operational activities are legal. Many lower level 2 and level 1 answers barely considered this at all.